

Kirkham & Wesham Primary School Confidentiality Policy

Date Policy Updated: October 2026

Review Date: October 2027

Purpose

This policy applies to all employees, volunteers, governors, agency staff, contractors, students on placement and any other individuals working on behalf of Kirkham & Wesham Primary School.

Kirkham & Wesham Primary School is committed to maintaining appropriate levels of confidentiality whilst ensuring that information is shared where necessary to safeguard children, comply with legal obligations and support the effective operation of the school. All staff and volunteers are expected to respect and protect confidential information obtained through their role.

Legal Framework

This policy is based on:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Keeping Children Safe in Education (KCSIE)
- Relevant safeguarding legislation and statutory guidance

The school processes personal data in accordance with data protection legislation and recognises that individuals have rights regarding how their information is collected, used, stored and shared.

Confidential Information

Confidential information includes, but is not limited to:

- Pupil records and assessment information
- Safeguarding and child protection information
- Special Educational Needs and Disabilities (SEND) information
- Medical and health information
- Staff employment records
- Performance management and disciplinary matters
- Payroll and financial information
- Information relating to parents, carers and families
- Any personal data that is not publicly available

Confidential information may be written, electronic, verbal or visual.

Staff and Volunteer Responsibilities

All staff and volunteers must:

- Treat all personal and confidential information with respect.
- Only access information required to carry out their duties.
- Not disclose confidential information to unauthorised persons.
- Ensure conversations regarding pupils, staff or families take place in appropriate settings.
- Keep passwords secure and not share login details.
- Lock computers when unattended and securely store paper records.
- Follow the school's data protection, acceptable use and online safety policies.
- Immediately report any suspected data breach, loss of information or unauthorised disclosure.

Confidential information obtained through work at the school must not be discussed outside the workplace, including with family members, friends or on social media.

Data Protection and GDPR

Personal data must be processed in accordance with the principles of UK GDPR.

Information must be:

- Processed lawfully, fairly and transparently.
- Collected for specified and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as required.
- Stored securely and protected against unauthorised access, loss or disclosure.

Staff and volunteers must only use personal data for authorised school purposes and must not retain copies of school data for personal use.

Safeguarding and Information Sharing

All staff should understand that safeguarding children is everyone's responsibility. Information relating to a child's welfare or safety may need to be shared with designated safeguarding staff, social care, the police or other appropriate agencies. In such circumstances, the need to protect a child overrides normal expectations of confidentiality.

Staff and volunteers must never promise a child that information disclosed to them will be kept secret. Concerns relating to the safety or welfare of a child must be reported immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL in accordance with the school's Child Protection and Safeguarding Policy.

Information should be shared on a need-to-know basis and only where there is a lawful and legitimate reason to do so.

Breaches of Confidentiality

A breach of confidentiality may include:

- Discussing confidential matters in public areas.
- Sharing information with unauthorised individuals.
- Sending information to the wrong recipient.
- Losing school records or devices.
- Accessing records without a legitimate reason.
- Inappropriate use of social media involving school information.

All actual or suspected breaches must be reported immediately to the Headteacher and Data Protection Lead.

Monitoring and Compliance

Failure to comply with this policy may result in disciplinary action, withdrawal of volunteer status, termination of contracts and, where appropriate, referral to external agencies or regulatory bodies.

Confidentiality obligations continue after employment, volunteering or other engagement with the school has ended.