School's Access Control Policy

September 2025

Owner: Brent Council Data Protection Officer on behalf of Chalkhill Primary School

Review Date: September 2026

Contents

Policy

Chalkhill Primary School controls access to information on the basis of school and security requirements.

Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the school requirements met by the controls.

The security requirements of each school application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

The access rights to each application take into account:

- Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
- System access control – access to data processing systems is prevented from being used without authorisation.
- Data access control – persons entitled to use a data processing system and gain access only to the data to which they have a right of access.
- Personal data cannot be read, copied, modified, or removed without authorisation.
- The classification levels of information processed within that application, ensure that there is consistency between the classification levels, and access control requirements across the network(s).
- Data protection (UK GDPR) and privacy, legislation and contractual commitments regarding access to data or services.
- The ‘need to know’ principle (i.e. access is granted at the minimum level necessary for the role).
- Information Asset Owners should ensure that there are regular access reviews for the systems they are responsible for.
- Access to high-risk systems must be provided once a user’s information governance training has been checked.
- ‘Everything is generally forbidden unless expressly permitted’.

- Rules must comply with the school's Access to Information Rule Book, which must always be enforced and those that are only guidelines.
- Users must declare a conflict of interest in their access to their line manager so that appropriate access restrictions can be put in place.
- Prohibit user-initiated changes to information classification labels.
- Prohibit user-initiated changes to user permissions.
- Enforcing rules that require specific permission before enactment.
- Any privileges that users need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

Chalkhill Primary School has standard user access profiles for common roles.

Ensure all staff including contractors & temporary workers are aware of schools access control policies and procedures.

Use Role forms to monitor & log access controls for school employees - joiners, leavers and change in role.

Management of access rights across the network(s) are the responsibility of the school.

User access requests, authorisation, and administration are segregated as described.

User access requests are subject to formal authorisation, to periodic review and to removal. If a network account is dormant after 90 days, the account shall be suspended.

Regularly review users access right and adjust or move where appropriate, for example when an employee change's role or leaves the school.

For contractors or temporary workers, there should be an expiry date for access, which should match their contract period.

Any exceptions to this policy must be approved by the school's data protection officer.