Nexus Education Schools Trust

Access Control Policy

Date: June 2018

Review Date: June 2019

Access Control Policy

1. NEST *c*ontrols access to information on the basis of business and security requirements.
2. Access control rules and rights to applications, expressed in standard user profiles, for each user/group of users are clearly stated, together with the business requirements met by the controls.
3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.
4. The access rights to each application take into account:

4.1 Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.

4.2 System access control – access to data processing systems is prevented from being used without authorisation.

4.3 Data access control – persons entitled to use a data processing system gain access only to the data to which they have a right of access.

4.4 Personal data cannot be read, copied, modified or removed without authorisation.

4.5 The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and networks.

4.6 Data protection (EU GDPR) and privacy BS 10012:2017 PIMS legislation and any contractual commitments regarding access to data or services.

4.7 The ‘need to know’ principle (i.e. access is granted at the minimum level necessary for the role).

4.8 ‘Everything is generally forbidden unless expressly permitted’.

4.9 ICT Department or IT Consultant prohibit user initiated changes to information classification labels

4.10 ICT Department or IT Consultant prohibit user initiated changes to user permissions.

4.11 ICT Department or IT Consultant enforce rules that require specific permission before enactment.

4.12 Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5. NEST has standard user access profiles for common roles in the Trust.
6. Management of access rights across the network(s) are agreed by the Headteacher of each NEST school and administered by the IT provider.
7. User access requests, authorisation and administration are segregated.
8. User access requests are subject to formal authorisation, to periodic review and to removal.