HIGH SPEED RAIL

The National College

National College for High Speed Rail
ACCESS CONTROL POLICY

Document Reference	NCHSR-GDPR-AC
Version	V1.0
Author	Daryl Unitt
Owner	Head of ICT & Facilities
Workstream / Business area	GDPR Working-Group
Classification	Public
Approval Level	SMT
Version approval date	23rd May 2018
Review schedule	Annually
Next review date	May 2019

1 The National College for High Speed Rail controls 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:
   a. Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
   b. System access control – access to data processing systems is prevented from being used without authorisation.
   c. 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.
   d. Personal data cannot be read, copied, modified or removed without authorisation.
   e. 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 network.
   f. Data protection (EU GDPR) and privacy, legislation and any contractual commitments regarding access to data or services.
   g. The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).
   h. 'Everything is generally forbidden unless expressly permitted'.
   i. Rules that must always be enforced such as Acceptable Usage
   j. Prohibit *[how?]* user initiated changes to information classification labels (see **Information Security Classification Guidelines**).
   k. Prohibit *[how?]* user initiated changes to user permissions.
   l. Enforcing *[how?]* rules that require specific permission before enactment.
   m. 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 The National College for High Speed Rail has standard user access profiles for common roles in the College (see **Access Control Rules and Rights for Users and User Groups**).
6 Management of access rights across the network(s) is via the New Starter, Leaver and Change Role/Access Procedure.
7 User access requests, authorisation and administration are segregated as described in **Access Control Rules and Rights for Users and User Groups**.
8 User access requests are subject to formal authorisation, to periodic review and to removal.