National College for High Speed Rail
INFORMATION SECURITY POLICY

Document Reference	NCHSR-GDPR-IS
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

The all staff and levels of management of The National College for High Speed Rail located at 2 Lister Street, Birmingham, West Midland. B7 4AG, which operates in the Education Sector in the business of providing Education, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with The National College for High Speed Rail's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

The National College for High Speed Rail's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in *[location/document/software]* and are supported by specific documented policies and procedures.

The National College for High Speed Rail aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of The National College for High Speed Rail are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, will receive appropriate training. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

The National College for High Speed Rail has established an Information Security Group, chaired by the DPO to support the ISMS review security policy

The National College for High Speed Rail is committed to achieving compliance with the GDPR.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security awareness training and more specialised Employees/Staff will receive appropriately specialised information security training.

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be

resilient and The National College for High Speed Rail must be able to respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to The National College for High Speed Rail's information and its systems.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data backup plans and security incident reporting. The National College for High Speed Rail must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of The National College for High Speed Rail including, but not limited to, computer hardware, data cabling, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and tablets, as well as on USB sticks and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

of Organisation Name.

The National College for High speed Rail

The ISMS is the Information Security Management System, of which this policy and other supporting and related documentation is a part.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the The National College for High Speed Rail