



INFORMATION SECURITY & DATA PROTECTION POLICY

The Costain Group is committed to managing all information in accordance with legislation, best practice and ISO 27001:2013.

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory and contractual obligations.

To achieve this, it is Costain's policy to ensure that:

- Information will be protected from unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information is made available only to authorised persons
- Information security training will be available to all staff
- All breaches of information security, actual or suspected, will be reported, investigated and resolved

The overall objective is to treat information appropriately and in accordance with the risks associated with it.

Personal data will be handled in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 ("Data Protection Legislation"). Data Protection Legislation regulates the capture, storage and use of information about individuals, known as "personal data".

To achieve compliance with Data Protection Legislation, Costain will ensure that:

- There are individuals in the organisation who can provide advice and assistance on issues arising under the Data Protection Legislation;
- Everyone managing and handling personal data understands that they are responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained;
- Queries about handling personal data are promptly dealt with;
- Procedures for handling personal data are clearly described; and
- A regular review is made of the way personal data is managed.

This policy applies to anyone that accesses Costain information and it should be read in conjunction with the ICT Acceptable Use Policy.

This policy will be reviewed annually to ensure the management of information security is suitable, effective, consistently implemented, and continually improved.

Signed:

A handwritten signature in black ink, appearing to read "A. Vaughan".

Date: 04/01/21.

A Vaughan (Chief Executive Officer)