Datagraphic

Information Security

Policy

Datagraphic

Information Security Policy

Document Information

Version:	2.2
Status:	LIVE
Issue date:	06/01/2026
Classification:	Public
Approved by:	Glyn King – CEO Robert Hoon – Group Managing Director
Author:	Mike Green – Chief Information Security Officer (CISO)
Owner:	Information Security Steering Committee (ISSC)

- A controlled document forming part of the Datagraphic ISO 27001 Information Security Management System (ISMS). All revisions must be made following the document control requirements of the standard.
- Effective from the Version and Issue date above. It supersedes previous versions, which are withdrawn and hard copies destroyed.
- Effective for Datagraphic Limited and Datagraphic Group Limited (hereafter referred to as “Datagraphic”).
- Uncontrolled when printed. The ‘master’ document is available under Datagraphic’s ISO 27001 ISMS Documentation Control Log.
- Subject to change by Datagraphic in line with changes in statutory law, case law and best practice.

Information Security Policy

Objectives

1. Ensure the protection of the confidential data under our control, including personally identifiable Information.

2. Ensure our products and services remain available and secure.

3. Ensure our network infrastructure remains available and secure.

4. Ensure our continued compliance with current UK laws, regulations and best practice guidelines.

5. Maintain controls that protect Information and Information systems against theft, abuse and other forms of harm and loss.

6. Minimise the risk of security incidents by ensuring our employees understand their Information Security responsibilities.

7. Continue to comply with ISO 27001 controls according to our certified Statement of Applicability.

8. Remain committed to the continual improvement of the Information Security Management System (ISMS).

The purpose of the Policy is to **protect Information assets**[1] from all threats, whether internal or external, deliberate or accidental.

The CEO & Managing Director have approved this Information Security Policy.

It is the policy of Datagraphic to ensure that:

- Information will be protected **against unauthorised access**
- **Confidentiality** of Information will be assured.[2]
- **Integrity** of Information will be maintained.[3]
- **Availability** of Information is ensured as required by the business processes.
- **Regulatory** and **legislative** requirements will be met.[4]
- **Business Continuity plans** will be in place, maintained and tested.[5]
- **Information Security training** will be available to all staff.[6]
- **All Information Security breaches**, actual or suspected, must be reported to line managers and investigated, if appropriate, by the CISO. [7]
- Datagraphic has an **Information Security Management System (ISMS)** to address the requirements of ISO 27001 and Pay.UK Standard 55 control objectives.* (*Standard 55 applies at the Datagraphic production facility only).
- **Business requirements** for the availability of Information and Information systems will be met.
- The CISO has responsibility for maintaining the Policy and providing advice and guidance on its implementation.
- **All managers** are directly responsible for implementing the Policy within their business areas and for adherence by their staff.

Procedures and policies exist to support the Policy and are maintained as an Information Security Management System (ISMS).

It is the responsibility of each staff member to adhere to the Policy.

Signed:

Robert Hoon
Group Managing Director

Signed:

Glyn King
CEO

Date: 06/01/2026

The CISO will review this Policy on an annual basis.

Footnotes:

1. Information takes many forms and includes data stored on computers, transmitted over networks (such as email and SFTP), printed out or written on paper, or spoken in conversation or over the telephone.
2. The protection of valuable or sensitive Information from unauthorised disclosure.
3. Safeguarding the accuracy and completeness of Information by protecting against unauthorised modification.
4. This applies to the requirements of Pay.UK (at the production centre), and the requirements of legislation such as the Data Protection Act 2018 and the UK GDPR.
5. This will ensure that Information and vital services are available when and where needed.
6. Staff will receive Information Security Awareness training upon inception and regularly after that, as appropriate to their job function.
7. Mike Green (CISO) – mgreen@datagraphic.co.uk

Document History

Date	Version	Author	Description of change
01/11/2011	1.1	M Green	Document created.
21/12/2014	1.2	M Green	Objectives added.
21/03/2018	1.3	M Green	Objective 8 added: Commitment to Continual Improvement added.
09/01/2019	1.4	M Green	Reviewed and re-signed by both Managing Directors.
02/01/2020	1.5	M Green	C&CCC updated to Pay.UK. Review and re-signed by both Managing Directors.
21/01/2021	1.6	M Green	Reviewed and re-signed by both Managing Directors.
26/01/2022	1.7	M Green	Reviewed and re-signed by both Managing Directors.
16/02/2022	1.8	M Green	Text changes are shown in bold below: All breaches of Information Security, actual or suspected, must be reported to **line managers** and investigated, **if appropriate**, by the Chief Information Security Officer (CISO). [7] This applies to the requirements of Pay.UK (at the production facility), and the requirements of legislation such as the Data Protection Act **2018** and the **UK** GDPR. Staff will receive Information Security training upon inception and **regularly** after that, as appropriate to their job function. Reviewed and re-signed by both Managing Directors.
01/04/2022	1.9	M Green	Reviewed and updated to the standard format.
06/06/2023	2.0	S Beech	Reviewed and re-signed by both Managing Directors.
07/02/2025	2.1	S Beech	Reviewed and signed by senior management.
06/01/2026	2.2	S Beech	Reviewed and signed by the senior management.

Questions

If you have questions about the contents of this policy, please contact:

Mike Green
CISO

E: issc@datagraphic.co.uk

Datagraphic

Certified B Corporation