Algospark Information Security Policy

Version: 0.02
Last updated: 7 June 2019
By Darren Wilkinson

Introduction
This information security policy outlines Algospark's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

Algospark is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Algospark is responsible.

Algospark is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001.

Objectives
The objectives of this policy are to:

a) Provide a framework for establishing suitable levels of information security for all Algospark information systems (including but not limited to all Cloud environments commissioned or run by Algospark, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
    a. This explicitly includes any ISO27001-certified Information Security Management Systems the School may run.
    b. The resources required to manage such systems will be made available
b) Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
c) Provide the principles by which a safe and secure information systems working environment can be established for staff, students and any other authorised users.
d) Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
e) Protect Algospark from liability or damage through the misuse of its IT facilities.
f) Maintain confidential information provided by clients and suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
g) Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

Scope
This policy is applicable to, and will be communicated to, all staff and third parties who interact with information held by the Algospark and the information systems used to store and process it. This includes, but is not limited to: Cloud systems developed or commissioned by Algospark, any systems or data attached to the Algospark data or telephone networks, systems managed by Algospark, mobile devices used to connect to Algospark networks or hold Algospark data, data over which Algospark holds the intellectual property rights, data over which Algospark is the data controller or data processor, electronic communications sent from the Algospark.

Information Security Principles
The following information security principles provide overarching governance for the security and management of information at Algospark.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements.
2. Staff with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. a. On this basis, access to information will be on the basis of *least privilege* and *need to know*.
5. Information will be protected against unauthorized access and processing in accordance with its classification level.
6. Breaches of this policy must be reported.
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of internal audits and penetration testing.
8. Any systems will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001 clause 10.

Legal & Regulatory Obligations
Algospark has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements. A non-exhaustive summary of the legislation is provided in the Appendix.

Information Classification
The following table provides a summary of the information classification levels that have been adopted by Algospark and which underpin the 8 principles of information security defined in this policy.
These classification levels explicitly incorporate the General Data Protection Regulation's definitions of Personal Data and Special Categories of Personal Data, as laid out in Algospark's Data Protection Policy, and are designed to cover both primary and secondary research data.

Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the Data Classification and Handling Guidlines.

	Public Data	Confidential Data	Sensitive Data	Secret Data
Description	Info that requires no protection: open and unclassified; likely to already exist in public domain. Examples: ads, press releases, blog posts, published info.	Info only available to staff to carry out roles. Examples: non-sensitive personal data, policies & processes, tenders, bids, proposals	Personal data, commercial data, legally privileged or under embargo. Examples: personal data, research, usernames, passwords, payment details, financial data, medical info, info under embargo.	Official secrets or data with potential to cause catastrophic harm. Example: obtained under Official Secrets Act or equivalent obtained as part of project.
Impact if info made public	None	Low: minor reputational or financial damage; minor privacy breach for individual	Medium: substantial reputational or financial damage; substantial privacy breach for individual	High: significant reputational or financial damage; distressful privacy breach for individual

Suppliers
All Algospark's suppliers will abide by Algospark's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:
- When accessing or processing Algospark assets, whether on site or remotely
- When subcontracting to other suppliers.

Cloud Providers
Where Algospark user Cloud services, Algospark retains responsibility as the data controller for any data it puts into the service.

- Cloud services used to process personal data will be expected to have ISO27001 certification, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.
- Any request for exceptions will be considered by the Risk Manager and the Chief Operating Officer.

Compliance, Policy Awareness and Disciplinary Procedures
All current staff and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines. Any security breach will be handled in accordance with all relevant policies, including the *Conditions of Use of IT Facilities at the Algospark* and the appropriate disciplinary policies.

Incident Handling
If any staff, client or supplier is aware of an information security incident then they must report it to the info@algospark.com or telephone +442075588728. Breaches of personal data will be reported to the Information Commissioner's Office by Algospark's Data Protection Officer.

Review and Development
This policy, and its subsidiaries, shall be reviewed by the Data Protection Officer and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas. The Data Protection Officer will determine the appropriate levels of security measures applied to all new information systems.

Responsibilities
- **Members of Algospark:** All members of Algospark, Algospark associates, agency staff working for Algospark, third parties and collaborators on Algospark projects will be users of Algospark information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so.

- **Data Controllers:**
  a) Members of Algospark will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:
  b) Project Managers / Project Leads: Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.
  c) Protection Officer: Responsible for Algospark's Data Protection Policy, data protection and records retention issues. Breach reporting to ICO
  d) Information Technology Committee: Responsible for approving information security policies.

Appendix

The Computer Misuse Act 1990
Defines offences in relation to the misuse of computers as:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

The Freedom of Information Act 2000
A general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996
“Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm”.

Obscene Publications Act 1959 and 1964
The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it.

Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008 & The Protection of Children Act 1978 prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs

Terrorism Act 2006
The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

Counter-Terrorism and Security Act 2015 – Statutory Guidance
The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales.

General Data Protection Regulation
The GDPR reinforces and extends data subjects’ rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover. The GDPR requires Algospark to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt out. It requires data breaches to be reported to the Information Commissioner’s Office within 72hrs of becoming aware of their existence.