BRIGHTMINDED

INFORMATION SECURITY POLICY

Last updated: 02 March 2026

- C O N F I D E N T I A L -

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of BrightMinded. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for BrightMinded to recover.

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

BrightMinded 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 BrightMinded is responsible.

BrightMinded is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of our clients or other third parties.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all BrightMinded information systems (including but not limited to all Cloud environments commissioned or run by BrightMinded, 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.

2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation.

3. Provide the principles by which a safe and secure information systems working environment can be established for staff or any other authorised users.

4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

5. Protect BrightMinded from liability or damage through the misuse of its IT facilities.

6. Maintain confidential information provided by clients or suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to, all staff and third parties who interact with information held by BrightMinded and the information systems used to store and process it.

This includes, but is not limited to: Cloud systems developed or commissioned by BrightMinded, any systems or data attached to the BrightMinded data or telephone networks, systems managed by BrightMinded, mobile devices used to connect to BrightMinded networks or hold BrightMinded data, data over which BrightMinded holds the intellectual property rights, data over which BrightMinded is the data controller or data processor, electronic communications sent from the BrightMinded network.

Supporting policies that form an integral part of this Information Security Policy are the BrightMinded Data Protection Policy and the BrightMinded Privacy Policy.

For the latest version of this and supporting policies, see https://brightminded.com/brightminded-information-security-policy/.

2. Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at BrightMinded.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 2.3. Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements (see *Section 2.2. Legal and Regulatory Obligations*).

2. Staff with particular responsibilities for information (see *Section 3. Responsibilities*) 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 (see *Section 1.2. Scope*) 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. On this basis, access to information will be on the basis of *least privilege* and *need to know*.

5. Information will be protected against unauthorised access and processing in accordance with its classification level.

6. User accounts must be secured with strong, unique passwords. Multi-factor authentication (MFA) will be enforced for internal and third-party systems whenever possible.

7. Breaches of this policy must be reported (see Sections *2.7. Compliance* and *2.8. Incident Handling*).

8. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits.

2.2 Legal & Regulatory Obligations

BrightMinded has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of contractual requirements. They have all been considered in the drafting of this policy. On-going changes to relevant legislation and contractual requirements are monitored by the Information Security Committee.

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by BrightMinded and which underpin the 8 principles of information security defined in this policy.

These classification levels explicitly incorporate the UK General Data Protection Regulation's definitions of *Personal Data* and *Special Categories of Personal Data*, as laid out in BrightMinded's *Data Protection Policy*[1].

Information may change classification levels over its lifetime, for example a client website can be classified as Confidential prior to go-live, but become Public after go-live.

Security Level	Definition	Examples
1. Confidential	Normally accessible only to specified members of BrightMinded staff. Should be held in an encrypted state outside BrightMinded systems; may have encryption at rest requirements from providers.	GDPR-defined *Special Categories* of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) from BrightMinded, clients or suppliers; passwords; large aggregates of personally identifying

[1] See BrightMinded's Data Protection Policy, the latest version of which can be found on https://brightminded.com/brightminded-information-security-policy/

		client data (>1000 records) including elements such as name, address, telephone number; Client requirements, designs, code.
2. Restricted	Normally accessible only to specified members of BrightMinded staff	GDPR-defined *Personal Data* (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs) from BrightMinded, clients or suppliers; BrightMinded financial data; other BrightMinded HR data; BrightMinded client and supplier legal contracts; any BrightMinded Board information; systems.
3. Internal Use	Normally accessible only to members of BrightMinded staff	internal correspondence; BrightMinded unreleased marketing information; information held under licence.
4. Public	Accessible to all members of the public	information available on the BrightMinded website or through

BrightMinded's social media channels.

2.4 Software security and cryptography

We subscribe to security updates issued by the maintainers of the operating systems and the software we use day to day. If and when new exploits are found and patches / upgrades are released we proceed with patching and / or updating our infrastructure appropriately as soon as reasonably possible and communicate an executive summary, with full disclosure of steps taken, to those of our clients whose operations may have been affected.

Appropriate encryption techniques for confidential information are through use of SSH keys that are at least 2048 bits, rsa and secured with a passphrase.

2.5 Suppliers

All BrightMinded's suppliers will abide by BrightMinded's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

• when accessing or processing BrightMinded assets, whether on site or remotely

• when subcontracting to other suppliers.

2.6 Cloud Providers

Under UK GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where BrightMinded uses Cloud services, BrightMinded retains responsibility as the data controller (or, if acting on behalf of clients as a data processor) for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. BrightMinded will also bear the responsibility for contacting the Information Commissioner's Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that BrightMinded is able to judge the appropriateness of a Cloud service provider's information security provision. This leads to the following stipulations:

1. 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.

2. Any request for exceptions will be considered by the Information Security Manager.

2.7 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of BrightMinded's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the UK General Data Protection Regulation, contravenes BrightMinded's Data Protection Policy, and may result in criminal or civil action against BrightMinded.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against BrightMinded. Therefore it is crucial that all users of BrightMinded's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.

All current staff and other authorised individuals will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines and will confirm agreement to adhere to the policies and any updates to them. Disciplinary consequences of non-adherence are at the discretion of the Information Security Committee.

2.8 Incident Handling

If a member of staff is aware of an information security incident, then they must report it to the Information Security Manager.

Breaches of personal data will be reported to the Information Commissioner's Office by BrightMinded's Information Security Manager.

2.9 Review and Development

This policy, and its subsidiaries, shall be reviewed by the Information Security Committee 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 Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3. Responsibilities

3.1 Members of BrightMinded:

All employees of BrightMinded, BrightMinded associates, agency staff working for BrightMinded, third parties and collaborators on BrightMinded projects will be users of BrightMinded 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. All staff and associates should therefore:

- ensure that any visitors they host are supervised at all times when in the main part of the office,
- always lock any device when away from the device, and
- be sensitive to unauthorised access by individuals gleaning information from a device while the staff member/associate is working on/using it.

Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see *Section 2.8: Incident Handling*

3.2 Data Controllers:

Some employees of BrightMinded will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

Software engineers / Project managers / Test QA: Responsible for the security of information produced, provided or held in the course of carrying out consultancy or development work for clients or on our own products. 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.

***Heads of Departments*:**

Responsible for the information systems (e.g. Sales, HR, Legal, Finance) both manual and electronic that support BrightMinded's work. Responsibilities as above (for *Software engineers / Project managers / TestQA*).

***Line managers*:**

Responsible for specific areas of BrightMinded work, including all the supporting information and documentation that may include working documents, contracts, or staff information.

Information Security Committee:

The BrightMinded management team acts as BrightMinded's Information Security Committee and is responsible for:

- This and subsequent information security policies and for providing advice on information security issues;
- BrightMinded's Data Protection Policy, Privacy Policy, data protection and records retention issues; and
- Physical aspects of security and providing advice on physical security issues.

Information Security Manager:

The Information Security Manager role rotates in the Information Security Committee and is currently (2026) held by Cristiano Solarino. The Information Security Manager is responsible for:

- Handling information security incidents;
- Determining the appropriate levels of security measures applied to all new information systems; and
- Breach reporting to ICO.

4. Cyberessentials miscellanea

This section enumerates BrightMinded policies related to Cyber Essentials Certification Compliance. Documentation on Cyber Essentials compliance can be found here.

Each section that follows addresses the corresponding section of the Cyber Essentials Compliance self-assessment.

4.1 Definitions

4.1.1 Scope

This is the part of the organisation and its operations that BrightMinded singles out for Cyber Essentials certification compliance. The scope includes BrightMinded's office, the infrastructure network (Digital Ocean, AWS etc) and the end users accessing it. It excludes the development network.

End users in scope are:

- Sam Griffin
- Dan Murray
- Cristiano Solarino
- Bradley Taylor

4.2 Policies

A4 Firewalls

A4.5 Firewall Management Process

If the eventuality occurs that an external process or service needs access to a currently restricted firewall port, a formal request must be submitted in an email to BrightMinded system administrator(s) (support@brightminded.com). The formal request must include:

- Firewall port to open
- Purpose of the request modification
- Length of time the modification is to be applied for
- Connecting service or process

The administrator(s) will review the application and either implement or deny the request.

A5 Secure Configuration

A5.1 Remove Unused Software

BrightMinded system administrators will review once per year the infrastructure stack and renew or update the list of services required on machines to effectively manage it.

It is the machine recipient's responsibility to make sure it complies with the list.

Should the need arise for a new software or plugin or extension, a formal request must be sent via email to sysadmin@brightminded.com for consideration. Requests must include:

- Software or service's name.
- Version if relevant.
- Purpose for the requested software or service.

A7 User Access Control

A7.4 User Privileges

BrightMinded staff are allocated specific user roles determining their access privileges with respect to every internal service or software they require access to for their day-to-day work. Should a staff member require modification of their current access privileges, they must issue a formal request via email (sysadmin@brightminded.com) to the system administrator(s). The request must include:

- Name of the service or software under consideration
- Access or privilege sought after
- Purpose of the permission update sought after

The administrator(s) will review the application and either implement or deny the request.

A7.13 Password Compromise Policy

In order to minimise risk when login credentials may have been compromised the following procedure is to be followed:

- Users must report suspected password compromise as soon as possible
- Upon notification:
    - The account is immediately secured (password reset or disabled)
    - Access logs are reviewed for unauthorised activity
    - Any affected systems are checked for malware
- Passwords must:
    - Be changed immediately using a newly generated 1password password
- Where MFA is available, it must be enabled
- The incident is logged and reviewed

This procedure is reviewed after any significant security incident.

Versioning

V1: 26/11/2018

V2: 15/02/2019

V3: 14/11/2022

V4: 24/02/2026

V5: 27/02/2026

V6: Current