DATA PROTECTION POLICY

General Statement of Octavius Hunt Ltd's Duties and Scope of this Policy
Octavius Hunt Ltd is required to process relevant personal data regarding members of staff, customers, business contacts, suppliers and other people the organisation has a relationship with or may need to contact as part of its operation. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Data Protection Law
Octavius Hunt Ltd will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

Octavius Hunt Ltd recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 and is actively working towards compliance with that directive.

The Principles
Octavius Hunt Ltd shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Personal Data
Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary. Personal data may also include sensitive personal data as defined in the Act.

Policy Scope
The policy applies to:

- The head office of Octavius Hunt Ltd
- All branches of Octavius Hunt Ltd
- All staff and volunteers of Octavius Hunt Ltd
- All contractors, suppliers and other people working on behalf of Octavius Hunt Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks
This policy helps to protect Octavius Hunt Ltd from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gains access to sensitive data.

Responsibilities
Everyone who works for or with Octavius Hunt Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.
- Octavius Hunt Ltd **will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords** must be used and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager if they are unsure about any aspect of data protection.

Data storage
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Operations Manager.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like CD, DVD or USB), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers, and should only be uploaded to an **approved cloud computing service**.

- Servers containing personal data should be **sited in a secure location**, away from general office space.

- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use
Personal data is of no value to Octavius Hunt Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption and theft:

- When working with personal data, employees should ensure the **screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be **encrypted before being transferred electronically**. IT support can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy
The law requires Octavius Hunt Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Octavius Hunt Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Octavius Hunt Ltd will make it **easy for data subjects to update the information** Octavius Hunt Ltd holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests
All individuals who are the subject of personal data held by Octavius Hunt Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations.**

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Operations Manager at info@octavius-hunt.co.uk.

The Operations Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Octavius Hunt Ltd will disclose requested data. However, the Operations Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information
Octavius Hunt Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, Octavius Hunt Ltd will provide a copy of this policy on request. A version of this policy is also available on the company's website www.octavius-hunt.co.uk/terms