1. Introduction :

Be Young Aesthetics needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

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.

2. Policy Statement & Purpose :

This data protection policy ensures that Be Young Aesthetics

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

3. Scope :

The Data Protection Act 1998 and 2018 describes how organizations, including Be Young Aesthetics must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

This policy applies to :

- All staff of Be Young Aesthetics.
- All contractors, suppliers and other people working on behalf of Be Young Aesthetics.
- All introducers and representatives working on behalf of Be Young Aesthetics.

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.

This can include:

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

4. Objective :

The Data Protection Act is underpinned by eight important principles. These say

that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

5. Policy Details :

This policy helps to protect Be Young Aesthetics 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 gained access to sensitive data.

6. Responsibilities :

Everyone who works for or with Be Young Aesthetics has some responsibility for ensuring data is collected, stored and handled appropriately.

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

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Be Young Aesthetics meets its legal obligations.

Be Young Aesthetics is responsible for:

1. Being updated about data protection responsibilities, risks and issues.
2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
3. Arranging data protection training and advice for the people covered by this policy.
4. Handling data protection questions from staff and anyone else covered by this policy.

7. 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.

Be Young Aesthetics 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 unauthorized 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 or the data protection officer if they are unsure about any aspect of data protection.

8. Data storage :

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

- When data is stored on paper, it should be kept in a secure place where unauthorized 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 unauthorized 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 unauthorized 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 a CD or DVD), 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 services.
- 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.

9. Data Use :

Personal data is of no value to Be Young Aesthetics 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 or 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. The IT manager can explain how to send data to authorized 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.

10. Data accuracy :

The law requires Be Young Aesthetics 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 Be Young Aesthetics 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.
- Be Young Aesthetics will make it easy for data subjects to update the information Be Young Aesthetics 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.

11. Subject access requests :

All individuals who are the subject of personal data held by Be Young Aesthetics 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 data controller at info@mc-aesthetics.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for their subject access request. The data controller will aim to provide the relevant data within 28 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

12. 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, Be Young Aesthetics will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

13. Providing information :

Be Young Aesthetics 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, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website. Be Young Aesthetics needs to ensure that the customer records can be made available for FCA inspection at any time.

Where records are stored electronically, they need to be reproduced, unchanged from their original content, stored so that they cannot be accidentally deleted and are regularly backed-up.

Staff should adhere to this policy when documents which contain sensitive data are destroyed appropriately, in accordance with the record keeping requirements listed.

14. Third Parties :

All third parties that share data and process data for us are referred to in this policy as "Partners" for convenience. They include any outsourced supplier such as Lead Introducers.

All Partners must undergo a due diligence process before data can be passed or shared to and from them. All Partners will undergo periodic audits; either desktop or office visits as determined by the outcome of the due diligence annually or as per their contracts. These will be stored in accordance with the Record Keeping Policy.

Only directors of Limited Liability companies will be asked to sign self-certification questionnaires. This is to mitigate the risk of general staff of Partners submitting data processing information during due diligence that could be inaccurate.

15. Consent :

Consent to collect, process and store data, must be collected from the individual that the data identifies. The consent must be freely given and not collected by an automatic acceptance such as submitting an enquiry and not being able to opt out. Consumers will be given the ability to opt out of marketing contact either verbally or online during the application process. Processing data is only legal if the consent captured is relevant to the processing we or our Partners carry out.

The consent collected will be recorded either by recorded call or in durable medium or electronic record. These will be stored in accordance with the Record Keeping Policy.

If the data collected is for marketing purposes and the marketing may be for services unrelated to the original consent given, then all purposes must be explained at the point of consent being given. Once the consumer enters into a contractual agreement with us, we have the legitimate right to contact that customer for business purposes. In the event that no contract is entered into then the processing the data of those consumers can only be made if consent for marketing was given.

16. Processing :

Once consent has been given, the customer will be made aware of their rights, which includes what their data is processed for, who we share it with and how long we will process it and store it for. This information will be given to the consumer via various methods depending on how the consumer has made contact.

The Privacy Notice will be available online and on paper. Reference to the consumers rights and the Privacy Notice will be brought to the attention of all consumers that make enquiries to us.

We have a legitimate right to process data and share that data to satisfy the enquiry of the consumer only if the consumer has been made aware of this need. This need is explained in the Privacy Notice, it explains the circumstances under which we would share the data. I.E if a loan provider rejected the case but another provider could accept the case. If the consumer opts out of this option then the data would be not be shared.

The capturing of photographic ID is not deemed to be racial or ethnic collection (sensitive data) the sharing of this data is only to be processed for verification purposes unless we are required legally to share it.

17. Consumer Rights :

As well as the above list of information a consumer data protection rights also include:

• A right to access the data held on them and receive it free of charge and within 30 days/ 1 month. We do not hold vast amounts of data on a consumer; therefore we cannot use the waiver to only supply caches of data by request.

• When providing data in a SAR the rights of others who may be identified in the data should also be considered.

• We should use all means possible to identify the parties making a SAR and that they have a legal right to the data.

• A right to know why the data is being collected and the consequences if we failed to provide the data requested.

• The Data Controller should give consumers the ability to make requests on exercising his rights electronically.

• A right to amend data held on them.

• A right to be forgotten is the right to have his data deleted for marketing purposes after the business need of processing has been completed. This includes informing partners, that the data has been historically shared with.

• A right to opt out of marketing contact. We should place the data that cannot be processed further onto a database that acts as a storage area when retention of data must be made under separate legislation or the data should be clearly identified as " Do Not Process or Restricted" on its existing database.

• A right to set preferred contact methods.

• A right to expect when processing their data will cease or when processing may continue in line with the nature of his original enquiry.

• A right to expect that his data will be held securely and that sensitive data about his health or his children will be afforded a higher level of security.

• A right not to be identified if he makes a disclosure under the Public Interest Disclosure Act 1998

• A right to know how his activity online is tracked

• A right to be informed of his rights in a clear and open manner. We should use easily recognised icons to identify consumer rights, which will facilitate potential language issues.

• All a consumer's rights should be given to them at the point when we collect data or when they submit data such as an online application.

• A human and not automated decision trees make all decisions made concerning loan advice solutions.

General staff guidelines on policy :

1. The only people able to access data covered by this policy should be those who need it for their work.

2. Data should not be shared informally. When access to confidential information is required, staff can request it from their line managers.

3. We will provide training to all staff to help them understand their responsibilities when handling data.

4. Staff should keep all data secure, by taking sensible precautions and following the guidelines below.

5. Strong passwords must be used and they should never be shared.

6. Personal data should not be disclosed to unauthorized people, either within the company or externally.

7. Data for marketing purposes 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.

8. Staff should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.