



Data Protection (General Data Protection GDPR)
Policy (including security of assessment materials)

Contents

1. Policy statement
2. Purpose & scope
3. Who needs to know about this policy
4. Responsibilities
5. Data protection risks
6. Data storage
7. Data use
8. Data accuracy
9. Subject access requests
10. Security of data
11. Security of assessment materials
12. Disclosing data for other reasons
13. Learner data
14. Providing information
15. Retention and disposal of data
16. Publication of business information
17. Related policies

1. POLICY STATEMENT

A1 Education & Training is committed to a policy of protecting the rights and privacy of individuals (includes learners, staff, and others) in accordance with the Data Protection Act. The Business needs to process certain information about its staff, learners, and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programs of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

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. PURPOSE AND SCOPE

This data protection policy ensures The Business:

- 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. WHO NEEDS TO KNOW ABOUT THIS POLICY

This Policy applies to:

- The head office of A1 Education & Training Ltd
- All branches and future branches of The Business
- All staff and volunteers of A1 Education & Training
- All contractors, suppliers and other people working on behalf of the business

4. RESPONSIBILITIES

The General Data Protection Regulation (GDPR) describes how organisations – including The Business must collect, handle, and store personal information.

These rules must 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.

The data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully

Those responsible for processing personal data must make reasonable efforts to ensure that data

subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Be obtained only for specific, lawful purposes

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Be adequate, relevant, and not excessive

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. Be accurate and kept up to date

Data, which are kept for a long time, must be reviewed, and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by A1 Education & Training are accurate and up to date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify The Business of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of A1 Education & Training to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Not be held for any longer than necessary

(see Retention and Disposal of Data)

6. Processed in accordance with the rights of data subjects

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision-making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

7. Be protected in appropriate ways

(see Security of Data)

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Data must not be transferred outside of the European Economic Area (EEA) - the fifteen EU Member States together with Iceland, Liechtenstein, and Norway - without the explicit consent of the individual. Members of A1 Education & Training should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

This applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

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

Everyone who works for or with The Business 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.

However, these people have key areas of responsibility:

- The directors are ultimately responsible for ensuring that The Business meets its legal obligations.

The Directors, are responsible for:

- Keeping the management team updated about data protection responsibilities, risks, and uses.
- Reviewing all data protection procedures and related policies, in line with agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Dealing with requests from individuals to see the data The Business holds about them.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The external ICT provider, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

All staff are responsible for:

- 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.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- 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 or the data protection officer if they are unsure about any aspect of data protection.

Managers are responsible for:

- Arranging for access to any data is revoked when a staff member leaves the business.

5. DATA PROTECTION RISKS

This policy helps to protect A1 Education & Training 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. DATA STORAGE

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

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 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 a CD 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 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 back up 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.

7. DATA USE

Personal data is of no value to A1 Education & Training 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 unauthorised 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.

8. DATA ACCURACY

The law requires A1 Education & Training to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and end 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.

A1 Education & Training will make it easy for data subjects to update the information The Business holds about them.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be removed from the database.

It is the Directors responsibility to ensure marketing databases are checked against industry suppression files every six months.

9. SUBJECT ACCESS REQUESTS (SAR)

All individuals who are the subject of personal data held by The Business 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 contact the company requesting the information, this is called a subject access request (SAR).

SAR requests from individuals should be made by email, addressed to the data controller at info@a1-training.co.uk The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 4 weeks of receipt of the original request.

The data controller will always verify the identity of anyone make a subject access request before handing over any information.

10. SECURITY OF DATA

All staff is responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and

that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft, or damage to personal data. Staff and learners should take particular care when processing personal data at home or in other locations outside The Business campus.

12. SECURITY OF ASSESSMENT MATERIALS

A1 Education & Training understands its responsibility for the security of assessment materials. These will be handled and stored as follows:

For all exam papers and assessment materials -

- All staff will be provided with training and guidance on security measures to ensure all assessment paperwork is kept securely and confidentially.
- All exam papers and assessment materials will remain in a locked facility which is only accessible by Directors, Quality Lead and Exams Administrative lead.

For awarding body printed exam papers –

- Exam papers will remain in original packaging until use.
- Printed exam papers are to be kept secure and not be left unattended at any time.
- Invigilators will sign to confirm receipt of exam papers.
- All exam papers, used and unused, will be returned to the exams department by the Invigilator at the end of each exam.
- A lockable box or case will be used for transporting exam papers to different venues

For assessment materials -

- Learners written work that is due to be assessed or has been assessed will be stored on the organisations SharePoint, under a secure file which will only be accessible to staff who require access.
- Where electronic portfolios are used, all learners work will remain in the portfolio instead of on SharePoint.
- Any learners who have not used an electronic portfolio will have their assessment paperwork shared with awarding organisations EQA's through their online system which is only accessible by approved account holders.
- When sharing any assessment materials within the organisation, staff will only use their work emails and will only share what is required.

12. DISCLOSING DATA FOR OTHER REASONS

A1 Education & Training must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a

colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work-related matter. The important thing to bear in mind is whether disclosure of the information is relevant to, and necessary for, the conduct of business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of The Business concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (e.g. a learner/member of staff has consented to The Business corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the institution is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring);
4. Where disclosure of data is required for the performance of a contract

When members of staff receive enquiries as to whether a named individual is a member of The Business, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether an individual is a member of A1 Education & Training may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, The Business may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of A1 Education & Training " to avoid confirming their membership or their presence in or their absence from the institution.

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 The Business 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 advisors where necessary.

13. LEARNER DATA

Information provided by learners may be shared with other organisations for purposes of administration, the provision of career and other guidance and statistical and research purposes, relating to education, training, employment, and well-being.

Other organisations include the Department for Works and Pensions, Local and Combined Authorities in England, the Greater London Authority, the Higher Education Statistics Agency, the Higher Education Funding Council for England, educational institutions, and organisations performing research and 3 of 5 statistical work on behalf of the Department for Education, or partners of those organisations.

Learner data is also collected and supplied to the Learning Records Service, a part of the ESFA. This personal data is used by the ESFA to issue learners with a Unique Learner Number (ULN), and to create and maintain the Personal Learning Record.

Information held in the Personal Learning Record is shared with third parties such as providers of learning.

Further details of how this personal data is processed for these purposes are published for the Learning Records Service.

14. PROVIDING INFORMATION

A1 Education & Training aims to always 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

15. RETENTION AND DISPOSAL OF DATA

A1 Education & Training discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and learners. However, once a member of staff or learner has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Learners In general, electronic learner records containing information about individual learners are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

Departments should regularly review the personal files of individual learners in accordance with The Business Records Retention Schedule.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

16. PUBLICATION OF BUSINESS INFORMATION

All members of A1 Education & Training should note that the Business publishes several items that include personal data and will continue to do so. These personal data are:

- Internal Telephone Directory.
- Information in prospectuses (including photographs), annual reports, staff newsletters, etc.
- Staff information on the Business website (including photographs).

It is recognised that there might be occasions when a member of staff, a learner, or a lay member of A1 Education & Training, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, A1 Education & Training should comply with the request and ensure that appropriate action is taken

Please note that any subsequent changes to legislation/acts, along with subsequent clauses mentioned within the internal policies of the Business are superseded by such amendments.

17. EMPLOYEE DATA

Which sources and what Personal Data do we use?

When you join as an employee, we will collect, use and process any Personal Data you provide, such as the following categories of data:

- Data of the civil register (Name, First name, Birth date,)
- Contact details (professional and personal)
- Professional life (Job profile, Position name, Hire date, weekly hours, Job Classification, ...)
- Qualifications and education data (CVs, etc.)
- Financial and property information (IBAN, Bank ID Number, Revenues,)
- Data connection (logs activities)
- IT identifiable data (Corporate ID, IP address, user account, login, ...)
- Images and video
- National Insurance number
- Health data

What are the purposes of the processing of your Personal Data?

To fulfil your contract of employment and to provide efficient management of the Businesses activities, we use your Personal Data for the following purposes such as:

- **Personnel administration management**
 - Staff register
 - Organisational chart
 - Reporting and dashboard management
 - Time and attendance
 - Corporate catering
 - Endowments management
 - Business cards

- **Compensation and benefit management**
 - Payroll management
 - Salary policy management
 - Other benefits management
- **Professional career management and Mobility**
 - Performance and goals
 - Global mobility
 - Internal Recruiting
 - Competence management
 - Qualifications and education
 - Quality/professional authorisations and accreditations
- **Development and Training management**
 - E-Learning (Virtual Classroom,)
 - Professional development
- **Security**
 - Authorisation monitoring
 - User management
 - IT security management
 - Access badges
 - Security camera system (CCTV)
- **Travel**
 - Professional travel management
 - Travel expenses
- **Communication**
 - The Businesses social network
 - Event management
 - Surveys
 - Newsletters
- **Use of the Businesses tools, equipment, systems and facilities**
 - IT assets and network
 - IT requests and support management
 - Active directory
 - Professional email
 - Mobile devices management
 - The Businesses store applications
 - License software management
 - IT tools for processing
- **Ethics & Legal compliance to comply with applicable legal obligations, including responding to an authority or court order or discovery request**
 - Professional whistleblowing
 - Reporting of professional and ethics incidents
 - Corporate audits

- Litigation management
- IP rights management
- Company law duties and mandates management
- **Performance of business activities**
 - Business organisation and operations improvement
 - Project management
 - Procurement
 - sales and customer services
- **Health & Safety**
 - Work accidents
 - Safety awareness
 - Occupational health
 - Working environment assessment
- **Protecting us and others**
 - Where we believe it is necessary to investigate, prevent or act regarding illegal & non-compliant activities, suspected fraud, emergency and crisis management, risks management or situations involving potential threats to the safety of any person or violations of policies, directives and procedures.

What is the basis for processing of your Personal Data?

As a responsible company, we need a lawful basis for collecting and/or processing your data. We generally rely on several grounds (reasons) for our business processing.

We process your Personal Data in accordance with the provisions set out in the GDPR and the relevant applicable Data Protection Laws and Regulations. The legal basis for processing your Personal Data are:

1. To comply with contractual obligations.

When you subscribe to a particular service through the Website, Recruitment Recourses and Job Applications, the purposes of processing your Personal Data are primarily determined by that service and we will process your information so that we can provide that service to you.

2. As a result of your consent.

When you have consented to the processing of your Personal Data by us for certain services such as through the Website, Recruitment Recourses and Job Applications, you can withdraw consent at any time by following the instructions provided in the application process or by contacting us at info@aonetraining.org.uk. For further information on the right of withdrawal, please see below Section "Am I obliged to provide my Personal Data?"

3. Within the scope of a legitimate interest.

On occasion we may not need your consent to use your data, given our legitimate interest to do so but we must inform you that we do this; examples of this are:

- For Payroll, Pre-employment checks including DBS, Occupational Health and Company Benefits system.
- For the analysis and optimisation of the Website.
- For ensuring IT security and the IT operation of E.G.G.

- For prevention and investigation of criminal acts.

4. Based on the Businesses legal obligations or in the public interest.

The Business as any other company, is subject to legal obligations and regulations. In some cases, the processing of your Personal Data will be necessary for the Business in order to fulfil these obligations.

Who will receive your Personal Data?

- Authorised persons working for or on behalf of the Business;
- The Business and affiliates of the Business, on a need-to-know basis for the purposes as outlined in this Privacy Notice;
- Our agents, service providers and advisers (e.g. Third-party service providers and advisers providing the variety of products and services we need such as IT maintenance and support, procurement services, compliance and security services, etc.);
- Other authorised third parties in connection with a reorganisation or sale of the Businesses and/or assets;
- Law enforcement or government authorities where necessary to comply with applicable law.

How long will your Personal Data be stored?

We process and store your Personal Data for as long as is required to meet our contractual and statutory obligations. The retention of your Personal Data is determined by Data Protection Laws and Regulation and by our procedures or processes adopted in accordance with Data Protection Laws and Regulation.

Security

We use technical and organisational security measures to protect the data we have under our control against accidental or intentional manipulation, loss, destruction and against access by unauthorised persons.

Our security procedures are continually enhanced as new technology becomes available.

What are your rights and how to exercise them?

You may at any time exercise your data protection rights:

- **Right to access/obtain a report detailing the information held about you:** You have the right to obtain confirmation as to whether your Personal Data is being processed by the Business and if so, what specific data is being processed.
- **Right to correct Personal Data:** You have the right to change any inaccurate Personal Data concerning you.
- **Right to be forgotten:** In some cases, for instance, when the Personal Data is no longer necessary in relation to the Purposes for which they were collected, you have the right for your Personal Data to be erased.
- **Right to stop the processing of your data:** You have the right to restrict the processing of your Personal Data by the Business, for instance when the processing is unlawful and you oppose the erasure of your Personal Data. In such cases, your Personal Data will only be processed with your consent or for the exercise or defence of legal claims.
- **Right to data portability:** Under some circumstances provided by law, you have the right to receive the Personal Data concerning you in a structured, commonly used and machine-readable format and/or transmit those Personal Data to another data controller.
- **Right to object and to withdraw consent:** please see below section “Am I obliged to provide my Personal Data?”

To this effect, please contact the Business in writing either by e-mail at the following address: info@a1-training.co.uk or by writing to the addresses below, enclosing a copy of a document evidencing your identity.

Grange House, Lancaster Rd, Shrewsbury SY1 3JF

Am I obliged to provide my Personal Data?

You may at any time object to the processing of your Personal Data or where your consent is required, withdraw such consent by contacting us at info@aonetraining.org.uk; However, please note that if you withdraw your consent, you may not be able to access and use certain information, features or services.

To what extent will decision-making be automated?

As a matter of principle, we do not use fully automated decision-making processes. If we should use such processes in individual cases, we will if prescribed by law, specifically inform you of this and of your rights in this respect.

Will profiling take place?

As a matter of principle, your Personal Data will not be processed automatically with the objective of evaluating certain personal aspects (profiling). If we should process your Personal Data with the objective of conducting profiling, we will, if prescribed by law, specifically inform you of this and of your rights in this respect.

How can I contact the Business in respect of my Personal Data?

If you are unhappy with the way in which your Personal Data has been processed or should you have questions regarding the processing of your Personal Data, you may refer in the first instance to the Business Data Protection Officer, who is available for enquiries or complaints, at the following email address: info@aonetraining.org.uk or you can write to the address below:

Grange House, Lancaster Rd, Shrewsbury SY1 3JF

Can I ask for assistance to the competent authorities?

If you remain unsatisfied, then you have the right to apply directly to a Data Protection Supervisory Authority. Below is the relevant Supervisory Authority:

[ICO: Supervisory Authority UK](#)

Cookies

Certain Business Internal portals and apps contain cookies. Cookies are small files that may be downloaded on your device when you access and use some of our web applications. They allow to recognise your device and store information about your preferences or past actions. We use cookies to record the preferences of our users, to enable us to optimise the design of our web applications. They ease navigation and increase the user friendliness of websites and applications. Cookies also help us to identify the most popular sections of our IT solutions. This enables us to provide content that is more accurately suited to your needs, and in so doing improve our service. You can prevent cookies from being stored on your device by setting your browser to not accept cookies. The exact instructions for this can be found in the manual for your browser. You can delete cookies already on your device at any time. However, if you choose not to accept cookies that are strictly necessary for the provision of our services provided by our website, it may result in a reduced availability of such services.

Modification of the Privacy Notice

The Business will update this Privacy Notice from time to time to reflect the changes in our practices and services and to remain compliant to Data Protection Laws and Regulations. We will inform you of any substantial modification in how we process your Personal Data.

18. RELATED POLICIES

- Assessment and verification
- Complaints
- Confidentiality
- Equality and diversity
- Safeguarding