Dar-ul-Madinah
An Islamic School System

Data Protection Policy

Date of last review: July 2024
Date of next review: July 2025

Data Protection policy

Introduction

The Data Protection Act 2018 achieved Royal Assent on 23 May 2018. It implements the government's manifesto commitment to update the UK's data protection laws.

The Data Protection Act 1998 served us well and placed the UK at the front of global data protection standards. The 2018 Act modernises data protection laws in the UK to make them fit-for-purpose for our increasingly digital economy and society.

As part of this the 2018 Act applies the EU's GDPR standards, preparing Britain for Brexit. By having strong data protection laws and appropriate safeguards, businesses will be able to operate across international borders. This ultimately underpins global trade and having unhindered data flows is essential to the UK in forging its own path as an ambitious trading partner. We have ensured that modern, innovative uses of data can continue while at the same time strengthening the control and protection individuals have over their data.
The main elements of the 2018 Act are:

General data processing

- Implements GDPR standards across all general data processing.
- Provides clarity on the definitions used in the GDPR in the UK context.
- Ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained.
- Provides appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Sets the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf

Darul-Madinah UK is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act") as re-enacted at any point in time, which came into force on the 23rd May 2018. Darul Madinah will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other associates of Darul Madinah who have access to any personal data held by or on behalf of Darul Madinah , are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, Dar-Ul-Madinah UK has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however

it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

Dar-Ul-Madinah UK regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between Darul Madinah and those with whom it carries out business. Darul Madinah will ensure that it treats personal information lawfully and correctly.

To this end Darul Madinah fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018.

The principles of data protection

The Data Protection Act 1998 stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Data Protection Act 2018 also requires businesses to comply with the standards of the new Act

- The Act is a complete data protection system, so as well as governing general data covered by the GDPR, it covers all other general data, law enforcement data and national security data. Furthermore, the Act exercises a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection.
- Organisations which already operate at the standard set by the Data Protection Act 1998 should be well placed to reach the new standards.
- The Act means that UK organisations are best placed to continue to exchange information with the EU and international community, which is fundamental to many businesses.
- The Information Commissioner has been working to help businesses to comply with the new Act from 25th May 2018 and is taking a fair and reasonable approach to enforcement after that date.

- Effective data protection relies on organisations adequately protecting their IT systems from malicious interference. In implementing the GDPR standards, the Act requires organisations that handle personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks. For many organisations such measures include effective cyber security controls.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and sensitive personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive information

Dar-Ul-Madinah UK will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 days;

- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, Dar-Ul-Madinah will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within Darul Madinah 's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners employees or agents of Darul Madinah must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Darul Madinah , are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between Darul Madinah and that individual, company, partner or firm;
- Allow data protection audits by Darul Madinah of data held on its behalf (if requested);
- Indemnify Darul Madinah against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by Darul Madinah will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by Darul Madinah .

Implementation

Darul Madinah has an appointed Data Protection Officer. This officer will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Data Protection Officer. The Data Protection Officer will also have overall responsibility for:

- The provision of cascade data protection training, for staff within Darul Madinah .
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the authority, with the Data Protection Act.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Dar-Ul-Madinah UK is registered as such.

The Data Protection Act 1998 and 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end the designated officer will be responsible for notifying and updating the processing of personal data, within the organisation.

The Data Protection Officer will review the Data Protection Register with designated staff annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Chief Officer immediately.

Please also refer to
GDPR compliance Policy
Privacy Notice