Dar-ul-Madinah
An Islamic School System

Compliance with GDPR

Date of last review: July 2021
Date of next review: September 2022

Dar Ul Madinah Compliance with GDPR

This document will act as a policy for Dar Ul Madinah to implement in 2018. It will be reviewed and updated, if necessary, in December 2018 for implementation during the calendar year 2019. Onwards it will be reviewed every Year.

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU)

The governors of Dar Ul Madinah tasked themselves to ensure that they were GDPR compliant.

A list of tasks / requirements was first drawn up and agreed upon.

Tasks / Requirements

1. Conduct an information audit to map data flows
2. Review information audit and create and action plan
3. Document what personal data we hold
4. Identify lawful bases for processing and document them
5. Review how you ask for and record consent
6. Need systems to record and manage ongoing consent
7. Register with the Information Commissioner's Office.
8. Provide privacy notices to individuals
9. Have a process to recognise and respond to individuals' requests to access their personal data
10. Have processes to ensure that the personal data you hold remains accurate and up to date
11. Have process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it
12. Have procedures to respond to an individual's request to restrict the processing of their personal data
13. Have processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability
14. Have procedures to handle an individual's objection to the processing of their personal data
15. Identify whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.
16. Have an appropriate data protection policy
17. Have a written contract with any data processors you use
18. Manage information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively
19. Have implemented appropriate technical and organisational measures to integrate data protection into your processing activities
20. We need policy and procedure which enable us to understand when you must conduct a DPIA and has processes in place to action this
21. Must have nominated a data protection lead or Data Protection Officer (DPO).
22. Decision makers and key people in your business need to demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business
23. Have an information security policy supported by appropriate security measures.
24. Ensure an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.
25. Have effective processes to identify, report, manage and resolve any personal data breaches

KEY

DPIA	Data protection impact assessments
DPO	Data Protection Officer

1. INFORMATION AUDIT AND DATA MAP FLOW

Personal data is collected by various means and for various reasons.

Dar ul Madinah has hired personnel to carry out various tasks. It also integrates with external companies to ensure the legal requirements are fulfilled.

The areas where data are collated are as follows.

1. Governor / Director Data
2. Employment data
3. Volunteers' data
4. Student details
5. Parents / Guardians details
6. CCTV Data
7. Visitors Book

Collecting data

1. **Governor / Director Data.**
   Governor data is held and stored in the head office on a password protected PC.
   Data stored is listed in section 3 and where documents are required e.g., passport copy, utility bills etc, no original documents are stored. Governors are requested to send scanned copies of these documents. Governor declaration forms are filled in and filed in head office

2. **Employment Data**
   Employees are requested to fill in application forms, banking details etc. This information is all scanned into the office 365 cloud system. Originals are kept at Admin office, copies at HR.
   This is all maintained by the HR department; however, some data are sent out from the HR department namely.
   a. Banking details to the finance department
   b. National insurance and personnel details to the accountant to generate wage slips etc

   Once all the data is scanned onto the cloud system, the hard copies are all filed and stored in the HR office.

3. **Volunteers Data**
   The data that we store on volunteers is not as extensive as paid employees. We do not require data for all volunteers as explained in section 3.

4. **Student Details**
   This data is stored in filing cabinets in the Nursery Manager's office in the building.

5. **CCTV**
   Dar Ul Madinah has CCTV in all of its buildings. The areas covered are as follows:
   a. Those areas where the general public attend
   b. Those areas where the students of the buildings attend
   c. Any offices where valuables or valuable data is stored

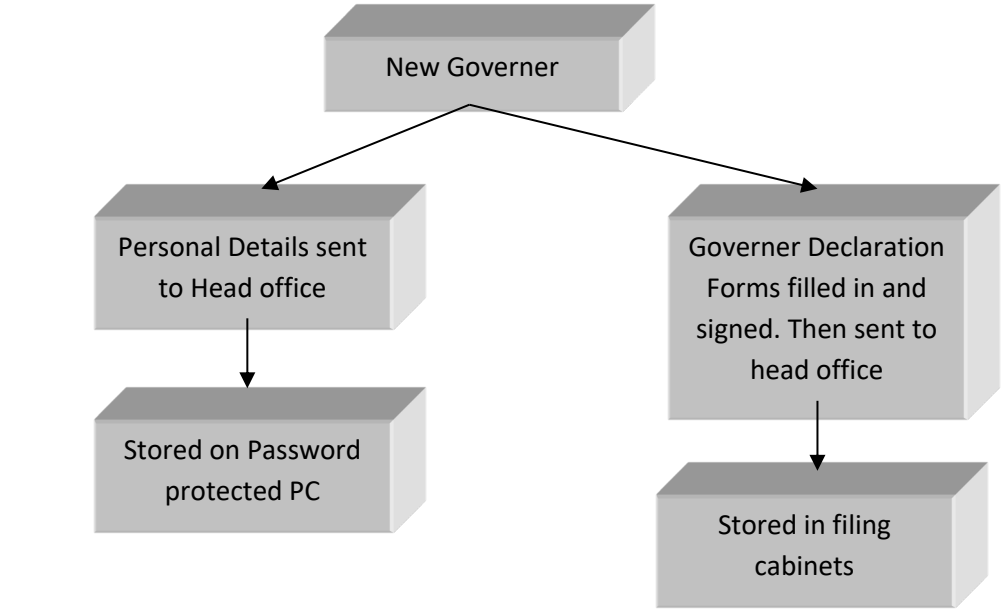
   All of our CCTV have retention systems where the Data is stored for 6 months.
   We do not share our control rooms with any third parties.
   All students are aware that CCTV recording is taking place.

6. **Parents / Guardians Details**
   Details are required for 2 reasons. One in the case of emergency and secondly in the case of early years funding where we need certain details of parents/ guardians to be able to claim this funding

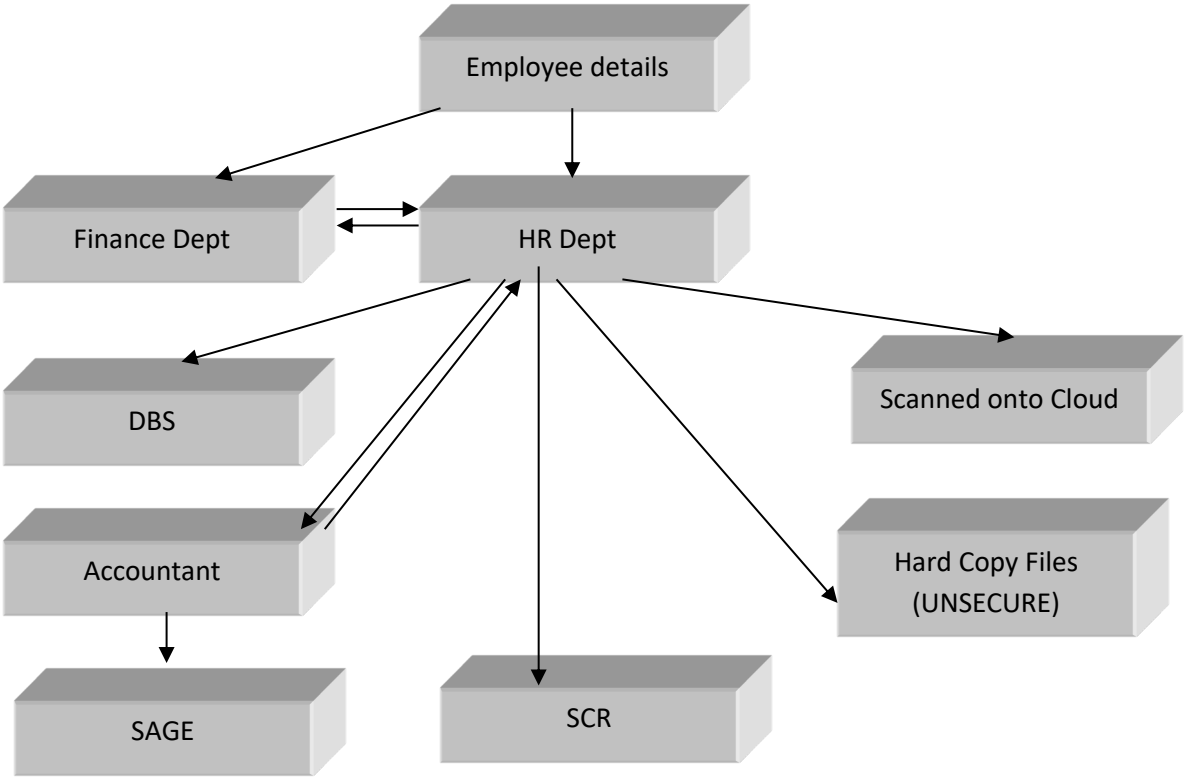
7. **Visitors Book**
   For safety reasons details of all visitors to the building are recorded.

Current Data Map Flow

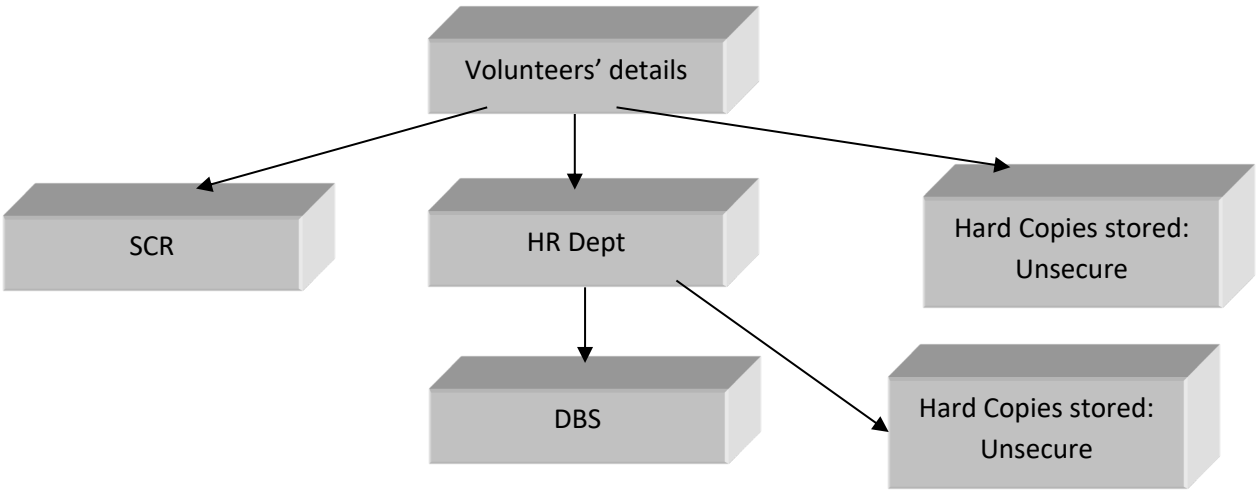
1. **Governor / Director Data**



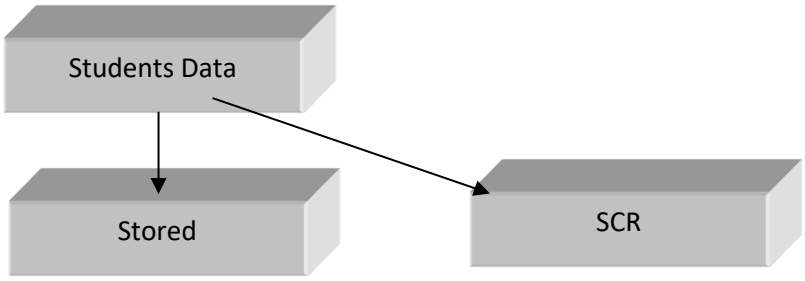
2. **Employment Data**



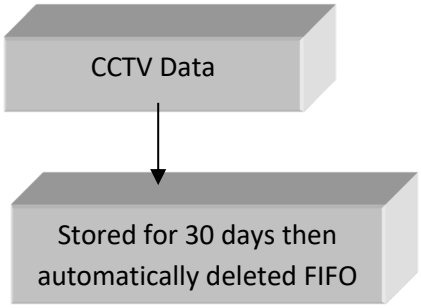
3. Volunteers Data



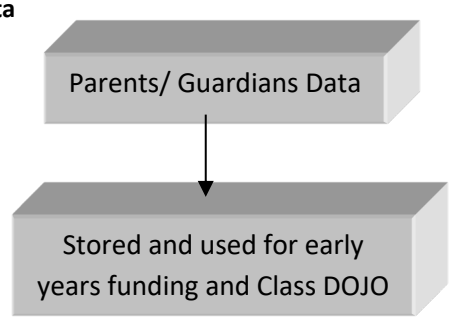
4. Students Data



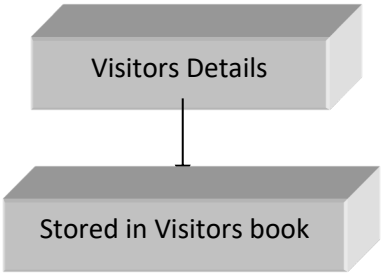
5. CCTV Data



6. Parents / Guardians Data



7. **Visitors Notebook**



2. INFORMATION REVIEW AND ACTION PLAN

A list of actions has been created which need to be implemented as soon as possible:

Data	Issue	Action
Governor / Director data	Saved on one PC in head office. Although password protected this PC could be stolen or fail to work	Server to be placed in head office. Data to be stored on this. Suitable backup to cloud created. Data removed from PC. Server and cloud to be password protected Password to be changed every 12 weeks.
Employment Data	Consent	Consent Forms need to be created and filled in by all workers
Employment Data	Data is being sent to the accountant so he can generate the wage slips.	Ensure the accountants company we use is GDPR compliant by getting a statement of them
Volunteers Data	Consent	Consent Forms need to be created and filled in by volunteers
Students Data	Consent	Consent Forms need to be created and filled in by all students
CCTV	Retention system	Policy to be put in place to ensure that retention system is checked periodically, and this check is recorded
Training	Awareness of GDPR	Training will be provided by the DPO to: Governor's HR Dept Finance Dept Head teachers and teachers Online training will also be sourced and provided to the above as backup to initial training. This is to be documented
Visitors Book	Details open	GDPR Compliant Visitors books to be used At end of each day visitors book to be locked away

3. PERSONAL DATA WE HOLD

Governor's

Governor information is kept on file and consists of

- Title
- Full Name
- Full address including postcode
- Email address
- Home Number
- Mobile Number
- Nationality
- Date Of Birth
- Place of Birth
- Country Of Birth
- Passport Copy
- Utility Bill

Employed Personnel

Whenever anybody joins the organisation as an employee or as self-employed then the following information is kept on that individual.

- Title
- Full Name
- Full address including postcode
- Email address
- Home Number
- Mobile Number
- Nationality
- Date Of Birth
- Place of Birth
- Country Of Birth
- Passport sized photo
- Previous address if not resident at current address for 5 years
- National Insurance Number
- Eligibility to work in UK
- Applicant is asked if they have a UK driving licence
- If so, how many point on licence
- Emergency Contact
- Name
- Relationship to applicant
- Address
- Home Number
- Mobile Number
- Email address
- Next of Kin
- Name
- Relationship to applicant
- Address
- Home Number
- Mobile Number
- Email address

- Health Status namely
- Have you been absent from work in last 2 years?
- If so, how many days
- Any medical conditions
- Disability Status
- Qualifications. If necessary, copies will be requested
- Employment Experience
- Offenders Status; namely
- Any previous convictions
- Any pending convictions
- If yes details of offence and sentence
- References (2 off). Info requested is
- Name
- Position
- Work Relationship
- Organisation
- Dates employed
- Address
- Mobile Number
- Email address

If applicant is successful, then the following information is also requested and kept on file. Some of this information is required for DBS checks whereas others for paying their wages

- Proof of ID. Passport preferred else right to work check is done
- Proof of address. Utility bill in name of applicant
- Bank details. Bank Name, account holder name, Sort Code, Account Number

Applicant is also required to sign a barred by declaration consent form. This is also kept on file

Volunteer Personnel

In the case of volunteers, the majority need to be DBS checked and as such the following data is kept on them

- Title
- Full Name
- Full address including postcode
- Email address
- Home Number
- Mobile Number
- Nationality
- Date Of Birth
- Place of Birth
- Eligibility to work in UK
- Applicant is asked if they have a UK driving licence
- If so, how many point on licence
- Emergency Contact
- Name
- Relationship to applicant
- Address
- Home Number
- Mobile Number
- Email address
- Proof of ID. Passport preferred else right to work check is done
- Proof of address. Utility bill in name of applicant

Students Data

The application form requests the following data

- Full Name
- Full address including postcode
- Email address
- Home Number
- Ethnicity
- Nationality
- Spoken Language (s)
- Parent / Guardians Details
- Academic education
- Medical Details, GP, and any history
- Emergency contact details
- Supplementary details namely
- Has the applicant had any serious illness or injuries?
- Has the applicant any known allergies?
- Has the applicant any known medical conditions?
- Has the applicant any particular or Special Needs?
- Following this the following data will be requested
- Proof of Address
- Copy of recent Nursery Report
- Two recent Passport Size photo's

Parents / Guardians Data

The application form requests the following data

- Full Name
- Full address including postcode
- Email address
- Home Number
- National Insurance Number

Victors Data

The following data is stored

- Full Name
- Date of visit
- Time of visit
- Time of departure
- Visiting who?
- Reason for visit

4. LAWFUL BASES FOR KEEPING DATA

Identify lawful basis for processing and document them

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

There are 6 lawful bases for processing data:

a. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d. **Vital interests:** the processing is necessary to protect someone's life.

e. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

With regards to Dar Ul Madinah:

a. **Consent:** the individual has filled in an application form, or has given information for a DBS check and as such has given consent

b. **Contract:** This applies to Dar Ul Madinah in relation to all employees

c. **Legal obligation:** for employment reasons and DBS checks we are legally obliged to keep this information

d. **Vital interests:** All employees and students are asked for emergency contact details so in the case of an emergency they can be contacted

e. **Public task:** This also applies to Dar Ul Madinah where for DBS checks which Is for the safety of all children and vulnerable adults then certain information is required from all employees and appropriate volunteers

f. **Legitimate interests:** This may not be applicable to Dar Ul Madinah

As such with regards to the data we collect:

1. **Governor Data**: this data is obtained under **consent** and is a **legal obligation**

2. **Employment data**: the data we hold is obtained under **consent** and is for **contract** purposes; it is **a legal requirement** and is also obtained for **vital interests** as well as for **public tasks**

3. **Volunteers' data**: the data we hold is obtained under **consent** and is for **public tasks**
4. **Student details**: the data we hold is obtained under **consent**; it is **a legal requirement** and is also obtained for **vital interests**

5. **CCTV Data**: this data is obtained as legal **obligation** as well **as vital interests**

6. **Parents / Guardians Details**: This is obtained under consent and the parent/guardians are aware of the reason for this

7. **Visitors' data**: This is obtained for **vital interests**

We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose.

We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

Where we process special category data, we have also identified a condition for processing special category data and have documented this.

Where we process criminal offence data, we have also identified a condition for processing this data and have documented this.

5. RECORDING CONSENT

With regards to the six areas where we collate data:

1. **Governor Data**
   The governor is aware that this data is being stored as he himself is providing this data for storage and future use

2. **Employment data**
   The employee is aware that this data is being stored as he himself is providing this data for storage and future use. Employment consent forms will also be created and filled in by all employees

3. **Volunteers' data**
   The volunteer is aware that this data is being stored as he himself is providing this data for storage and future use. Volunteer consent forms will also be created and filled in by all volunteers

4. **Student details**
   The parent / guardian is aware that this data is being stored as they are providing this data for storage and future use. Consent forms will be created and filled in

5. **CCTV Data**
   In the case of students, they are all aware of CCTV as it is part of the application from to provide consent for this.

6. **Parent / Guardian data**
   The parent / guardian is made aware of the reason for data ad at time of giving data it is explained to them the reasons for this. Consent forms will be created and filled in

7. **Visitors Data**
   The visitor data is given at their consent

6. ONGOING CONSENT

The areas where data is collated are as follows.

1. Governor Data
2. Employment data
3. Volunteers' data
4. Student details

5. CCTV Data
6. Parent / Guardians Details
7. Visitors Data

With regards to ongoing consent:

1. Governor Data
   The governor's data is checked every 6 months for accuracy and as such consent is automatically obtained as a result of this

2. Employment data
   The employee's data is checked every 6 months for accuracy and as such consent is automatically obtained as a result of this

3. Donor's data.
   Not applicable

4. Student detail
   The student's details data is checked every 6 months for accuracy and as such consent is automatically obtained as a result of this

5. CCTV Data
   Not applicable

6. Parents / Guardians Data
   New consent forms will be issued every time data is requested

7. Visitors Data
   Not applicable

7. INFORMATION COMMISSION OFFICE REGISTER

We have registered with the Information Commissioner's Office and our registration reference is available upon request.

8. PRIVACY NOTICES TO INDIVIDUALS

The following notice will be provided to all individuals that we take personal data of.

There are 6 lawful reasons for requesting data from individuals

They are as follows

a. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d. **Vital interests:** the processing is necessary to protect someone's life.

e. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

With regards to Dar Ul Madinah:

a. **Consent:** the individual has filled in an application form, or has given information for a DBS check and as such has given consent

b. **Contract:** This applies to Dar Ul Madinah in relation to all employees

c. **Legal obligation:** for employment reasons and DBS checks we are legally obliged to keep this information

d. **Vital interests:** All employees are asked for emergency contact details so in the case of an emergency they can be contacted

e. **Public task:** This also applies to Dar Ul Madinah where for DBS checks, which is for the safety of all children and vulnerable adults then certain information is required from all employees and appropriate volunteers

f. **Legitimate interests:** This may not be applicable to Dar Ul Madinah

As such as you can see above, we are obliged to acquire this data from you and process it and hold on record Please confirm if this is acceptable to you.

9. INDIVIDUALS REQUEST TO PERSONAL DATA

Overview
Individuals have the right to access their personal data and supplementary information.
The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing

Dar Ul Madinah will not charge a fee for the copy of information However, fees may be charged if a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information.

The fee will be based on the administrative cost of providing the information.

Timescales

Information will be provided without delay and at the latest within one month of receipt.

Dar Ul Madinah may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, Dar Ul Madinah will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, Dar Ul Madinah can and may:

Charge a reasonable fee considering the administrative costs of providing the information; or refuse to respond.

Where Dar Ul Madinah refuses to respond to a request, Dar Ul Madinah will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Dar Ul Madinah must verify the identity of the person making the request, using ‘reasonable means.

Data will not be provided to relatives or friends requesting on their behalf

If the request is made electronically, you should provide the information in a commonly used electronic format.

Where Dar Ul Madinah process a large quantity of information about an individual, the GDPR permits Dar Ul Madinah to ask the individual to specify the information the request relates to.

The GDPR does not include an exemption for requests that relate to large amounts of data, but Dar Ul Madinah may be able to consider whether the request is manifestly unfounded or excessive.

10. ACCURATE PERSONAL DATA

The areas where data is collated are as follows.

1. Governor Data
2. Employment data
3. Donor's data.
4. Student details
5. CCTV Data
6. Parents / Guardians Data
7. Visitors Data

With regards to ensuring the data that we hold is accurate:

1. Governor Data

The governors are requested to be proactive in updating details, however every 6 months the governor data is confirmed via email

2. Employment data

The employees are requested to be proactive in updating details, however every 6 months the employee data is confirmed via email

3. Volunteers' data

The volunteers on which we hold data are requested to be proactive in updating details, however every 6 months the volunteer data is confirmed via email

4. Student detail

The students on which we hold data are requested to be proactive in updating details, however every 6 months the student data is confirmed via email or letter to parent / guardians/students

5. CCTV Data

Not applicable

6. Parents / Guardians Data

This will be updated every academic year

7. Visitors Data

Not applicable

11. DISPOSAL OF PERSONAL DATA

The areas where data is collated are as follows.

1. Governor Data
2. Employment data
3. Donor's data.
4. Student details
5. CCTV Data
6. Parent / Guardian Data
7. Visitors Data

With regards to disposal of personal data:

1. Governor Data. Period that the individual acted as a governor will be kept on file indefinitely. Data other than this will be kept on records for 7 years after the individual is no longer a governor. Disposal will consist of company emails which will be deleted from server and cloud. Governor details and governor declaration which consists of hard copies and scanned copies will be disposed of. Hard copies will all be shredded before being disposed of

2. Employment Data. Period that the individual acted as an employee will be kept on file indefinitely. Data other than this will be kept on records for 7 years after the individual is no longer a governor. Disposal will consist of company emails which will be deleted from server and cloud. All other files which consist of hard copies and scanned copies will be disposed of. Hard copies will all be shredded before being disposed of

3. Volunteers Data. Data of volunteers is obtained for DBS purposes and as such there is no need to keep data on them once their DBS is expired and not renewed. Those that are renewed will automatically be stored. Files which consist of hard copies and scanned copies will be disposed of. Hard copies will all be shredded before being disposed of

4. Student Details. Details of study duration will be kept indefinitely. Other records will be disposed of after a period of 7 years. Files which consist of hard copies and scanned copies will be disposed of. Hard copies will all be shredded before being disposed of.

5. CCTV. Our storage systems store data for a fixed time and then are automatically deleted. Method of deletion is FIFO

6. Parents/ Guardians. Data will be retained indefinitely

7. Visitors Data:
   This data will be kept for a period of 3 years

12. RESTRICTING USE OF PERSONAL DATA

The areas where data is collated are as follows.

1. Governor Data
2. Employment data
3. Volunteers' data
4. Student details
5. CCTV Data
6. Parents / Guardians
7. Visitors Data

With regards to restricting the use of personal data.

1. Governor Data. The governor can request the restriction of personal data, but as such the remaining governors would then have to meet and discuss the implications of having a governor whose data we cannot process and as such it may not be feasible for the governor to continue in his post

2. Employment Data. As the data is only used for legal purposes the employee cannot request the restriction of use of his data. However, if the employee makes a reasonable demand, e.g., a female employee only wishes for females to process her data, and then where feasible this will be accommodated.

3. Volunteers Data. As the data is only used for legal purposes the employee cannot request the restriction of use of his data. However, if the employee makes a reasonable demand, e.g., a female employee only wishes for females to process her data, then where feasible this will be accommodated

4. Student Data. As the data is only used for legal purposes the employee cannot request the restriction of use of his data. However, if the employee makes a reasonable demand, e.g., a female employee only wishes for females to process her data, then where feasible this will be accommodated

5. CCTV. If a request is made and it is feasible without legal implications to accommodate then wherever possible the request will be fulfilled

6. Parents Data. As the data is only used for legal purposes the parent cannot request the restriction of use of his data. However, if the parent makes a reasonable demand, e.g., a female employee only wishes for females to process her data, then where feasible this will be accommodated

7. Visitors Data: As the data is only used for vital and legal purposes the visitors cannot request the restriction of use of his data. However, if the visitor makes a reasonable demand, then where feasible this will be accommodated

13. TRANSFER OF PERSONAL DATA

Currently the action plans it to update our current cloud server and possibly create a physical server in the head office. IT specialists will be brought in to survey the action and produce a risk assessment and a report. This report and risk assessment will need to be approved by governors prior to implementation.

If in the future this needs to be updated, then similar process will need to be undertaken to ensure safe transfer

14. OBJECTION OF USE OF PERSONAL DATA

The areas where data is collated are as follows.

1. Governor Data
2. Employment data
3. Volunteers' data
4. Student details
5. CCTV Data
6. Parents/ Guardians
7. Visitors Data

With regards to the objection of use of personal data;

1. Governor Data. The governor can object the use of personal data, but as such the remaining governors would then have to meet and discuss the implications of having a governor whose data we cannot process and as such it may not be feasible for the governor to continue in his post

2. Employment Data. As the data is only used for legal purposes the employee cannot object to the use of their data. However, if the employee makes a reasonable demand, e.g., a female employee only wishes for females to process her data, and then where feasible this will be accommodated.

3. Volunteers Data. As the data is only used for legal purposes the employee cannot object to the use of their data. However, if the employee makes a reasonable demand, e.g., a female employee only wishes for females to process her data, then where feasible this will be accommodated

4. Student Data. As the data is only used for legal purposes the student cannot request the restriction of use of his data. However, if the student makes a reasonable demand, e.g., a female student only wishes for females to process her data, then where feasible this will be accommodated

5. CCTV. If a request is made and it is feasible without legal implications to accommodate then wherever possible the request will be fulfilled

6. Parents/ Guardians. If a request is made and it is feasible without legal implications to accommodate then wherever possible the request will be fulfilled

7. Visitors Data: If a request is made and it is feasible without legal implications to accommodate then wherever possible the request will be fulfilled

15. AUTOMATED DECISIONS RE PERSONAL DATA

There are no automated processing operations, other than the automatic deletion of CCTV data
As such we do not need any procedures to deal with this.
However, our processes will be reviewed annually and every time we start a new process

16. DATA PROTECTION POLICY

The following is a copy of our Data protection policy which is part of our overall policies file

Introduction

Dar Ul Madinah is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act") as re-enacted at any point in time, which came into force on the 1st of March 2000. Dar ul Madinah will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners, or other servants of Dar ul Madinah who have access to any personal data held by or on behalf of Dar ul 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 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 regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between Dar ul Madinah and those with whom it carries out business. Dar ul Madinah will ensure that it treats personal information lawfully and correctly.

To this end Dar ul Madinah fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

The principles of data protection

The Act 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 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 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 Dar ul 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 or other servants or agents of Dar ul Madinah must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Dar ul 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 Dar ul Madinah and that individual, company, partner, or firm.
- Allow data protection audits by Dar ul Madinah of data held on its behalf (if requested).
- Indemnify Dar ul 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 Dar ul Madinah will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by Dar ul Madinah.

Implementation

Dar ul 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 Dar ul 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 is registered as such.

The Data Protection Act 1998 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.

17. DATA PROCESSORS CONTRACT

Dar Ul Madinah uses external companies to assist them with regards to certain activities.

This includes the accountant who will use our employee information to generate the wages and wage slips etc.
They will also have access to all of our accounts which will include receipts and invoices.

A written statement will be achieved from our accountant to ensure that they are GDPR compliant with any data that we provide them

18. INFORMATION RISKS

Purpose

Information that is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss, and corruption.

However, the implementation of controls to protect information must be based on an assessment of the risk posed to Dar Ul Madinah and must balance the likelihood of negative impact against the resources required to implement the controls, and any unintended negative implications of the controls.

This policy sets out the principles that Dar Ul Madinah uses to identify, access, and manage information risk, in order to support the achievement of its planned objectives, and aligns with the overall risk management framework and approach.

This high-level Information Risk Management Policy sits alongside the Information Security Policy and Data Protection Policy to provide the high-level outline of and justification for Dar Ul Madinah risk-based information security controls.

Objectives
Dar Ul Madinah's information risk management objectives are that:

1. our information risks are identified, managed, and treated according to an agreed risk tolerance
2. our physical, procedural, and technical controls are agreed by the information asset owner
3. our physical, procedural, and technical controls balance user experience and security
4. our physical, procedural, and technical controls are cost-effective and proportionate•

Scope

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all information used by Dar Ul Madinah, in all formats.

This includes information processed by other organisations in their dealings with Dar Ul Madinah.

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all individuals who have access to Dar Ul Madinah information and technologies, including external parties that provide information processing services to Dar Ul Madinah.

Compliance
Compliance with the controls in this policy will be monitored by the Information Security Manager and reported to the Information Security Board.

Review
A review of this policy will be undertaken by the Information Security Manager annually or more frequently as required and will be approved by the Dar Ul Madinah Governor's.
Policy Statement
Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset.
It is used to determine their impact and identify and apply controls that are appropriate and justified by the risks.

It is Dar Ul Madinah's policy to ensure that Information is protected from a loss of:

1. Confidentiality – information will be accessible only to authorised individuals
2. Integrity – the accuracy and completeness of information will be maintained
3. Availability – information will be accessible to authorised users and processes when required

1. Risk assessment
   Risk assessments must be completed with access to and an understanding of:
   a. Dar Ul Madinah's business processes• the impact to Dar Ul Madinah of risks to business assets
   b. the technical systems in place supporting the business
   c. the legislation to which Dar Ul Madinah is subject
   d. up-to-date threat and vulnerability assessments

A risk assessment exercise must be completed at least:

a. for every new information-processing system
b. following modification to systems or processes which could change the threats or vulnerabilities
c. following the introduction of a new information asset
d. when there has been no review in the previous three years
e. A risk score is calculated from Likelihood x Impact Level giving the results below, consistent with Dar Ul Madinah's high level Risk Management Policy

CRITICAL	5	10	15	20	25
MAJOR	4	8	12	16	20
MEDIUM	3	6	9	12	15
LOW	2	4	6	8	10
MINOR	1	2	3	4	5
IMPACT / LIKELIHOOD	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH

2. Threats

   Dar Ul Madinah will consider all potential threats applicable to a particular system, whether natural or human, accidental, or malicious.

   Dar Ul Madinah will reference Annex C of the ISO 27005 standard to aid with threat identification.

   Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

   It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations

3. Vulnerabilities

   Dar Ul Madinah will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

   Dar Ul Madinah will reference Annex D of the ISO 27005 standard to aid with vulnerability identification.

   Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

   It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations.

4. Risk Register

   The calculations listed in the risk assessment process will form the basis of a risk register. All risks will be assigned an owner and a review date.

   The risk register is held in the Information Security document store, with access controlled by the Information Security Manager.

5. Risk Treatment

   The risk register will include a risk treatment decision.

   The action will fall into at least one of the following categories:

   1. Tolerate the risk – where the risk is already below Dar Ul Madinah's risk appetite and further treatment is not proportionate
   2. Treat the risk – where the risk is above Dar Ul Madinah's risk appetite, but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below Dar Ul Madinah's risk appetite
   3. Transfer the risk – where the risk cannot be brought below Dar Ul Madinah's risk appetite with proportionate treatment, but a cost-effective option is available to transfer the risk to a third party
   4. Terminate the risk – where the risk cannot be brought below Dar Ul Madinah's risk appetite with proportionate effort/resource and no cost-effective transfer is available

      The Information Security Manager in collaboration with the Information Asset Owner will review Medium and Low risks and recommend suitable action.

      The Information Security Board in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

      In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

6. Roles and Responsibilities

   The Chair of the Information Security Board has accountability to the Governor's for managing information risk.

   They will direct the information risk appetite for Dar Ul Madinah and review the information risk register.

They will be involved in assessing and reviewing High risks via the Information Security Board.
The Information Security Manager is responsible to the Governor's for managing the risk assessment process and maintaining an up-to-date risk register.
The Information Security Manager will conduct risk assessments and recommend action for Medium and Low risks.
The Information Security Board is responsible for assessing and reviewing High risks and will have visibility of the risk register.
Information Asset Owners must be responsible for agreeing and implementing appropriate treatments to risks under their control.
They must also take an active role in identifying new risks

19. IMPLEMENTATION OF DATA PROTECTION

The various sections above have shown the methods and measures taken and to be taken to ensure that all the data within the organisation is secure

20. DPIA

Data protection impact assessments (DPIAs) help organisations identify, assess, and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

Why should a DPIA be conducted?

The GDPR mandates a DPIA be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". The three primary conditions identified in the GDPR are:

- A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale.

Examples of personal data processing where a DPIA is likely to be required

- A hospital processing its patients' genetic and health data on its information system.
- The archiving of pseudonymised personal sensitive data from research projects or clinical trials.
- An organisation using an intelligent video analysis system to single out cars and automatically recognise registration plates.
- A company systematically monitoring its employees' activities, including their workstations and Internet activity.
- The gathering of public social media data for generating profiles.
- An institution creating a national-level credit rating or fraud database.

The Article 29 Working Party (WP29), in its guidelines on DPIAs, sets out the criteria that organisations should consider when determining the risks posed by a processing operation. The more criteria that are met by processing, the more likely it is to present a high risk to the rights and freedoms of individuals, and therefore to require a DPIA

When should a DPIA be conducted?

A DPIA should be conducted as early as possible within any new project lifecycle, so that its findings and recommendations can be incorporated into the design of the processing operation.

Known as privacy by design, the embedding of data privacy features into the design of projects can have the following benefits:

- Potential problems are identified at an early stage.
- Addressing problems early will often be simpler and less costly.
- Increased awareness of privacy and data protection across the organisation.
- Organisations will be less likely to breach the GDPR.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Who should be involved in conducting a DPIA?

The organisation (data controller) is responsible for ensuring the DPIA is carried out.

The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team. If your organisation does not possess sufficient expertise and experience internally, you may consider bringing in external specialists to consult on or to carry out the DPIA.

Under the GDPR it is necessary for any organisation with a designated data protection officer (DPO) to seek the DPO's advice. This advice and the decisions taken should be documented as a part of the DPIA process.

21. GDPR TRAINING

The DPO (data Protection Officer) will use this document as the basis of training.
This training will be documented.

22. INFORMATION SECURITY POLICY

Introduction

Dar Ul Madinah recognises that Information is fundamental to its effective operation and next to staff, is its most important business asset.

The purpose of this Information Security Policy is to ensure that the information managed by Dar Ul Madinah is appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

Failure to adequately secure information increases the risk of financial and reputational loss to Dar Ul Madinah.

This overarching policy document provides management direction and support for information security and lists a set of component sub-policy documents which taken together constitute the Information Security Policy of Dar Ul Madinah.

Purpose

The objectives of this policy are to:

1. Ensure that all information and information systems within Dar Ul Madinah are protected to the appropriate level.
2. Ensure that all users are aware of and comply with this policy including sub-policies and all current and relevant UK and EU legislation.
3. Provide a safe and secure information systems environment for staff, students, and 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 Dar Ul Madinah from liability or damage through the misuse of information or information systems.

6. Ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

Scope

The Information Security Policy applies to information in all its forms, collectively termed 'information assets' within this document. It covers information in paper form, stored electronically or on other media, information transmitted by post, by electronic means and by oral communication, including telephone and voicemail.
It includes text, pictures, audio, and video.
It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.
Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory, or contractual obligations

This policy applies to all staff, students and other members of Dar Ul Madinah and third parties who interact with information held by Dar Ul Madinah and the information systems used to store and process it, collectively termed 'users' throughout this document.

For the purposes of this document, information security is defined as the preservation of:

Confidentiality (protecting information from unauthorised access and disclosure)

Integrity (safeguarding the accuracy and completeness of information)

Availability (ensuring that information and associated services are available to authorised users when required)

Information Security Principles

The following principles underpin this policy:

1. Information will be protected in line with all relevant Dar Ul Madinah policies and legislation.
2. It is the responsibility of all individuals to be mindful of the need for information security across Dar Ul Madinah and to be aware of and comply with this policy including sub-policies and all current and relevant UK and EU legislation.
3. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
4. All information will be classified according to a level of risk.
5. Information will be made available solely to those who have a legitimate need for access.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. The integrity of information will be maintained.
8. Information will be protected against unauthorised access.

Information Classification

The following table provides a summary of the risk-based information classification levels that have been adopted by Dar Ul Madinah.

CLASSIFICATION LEVEL	DESCRIPTION	EXAMPLES
HIGH	Loss, misuse, or unauthorised access to this data could result in significant financial loss, reputational loss, and litigation	Student data Staff data Financial data
MEDIUM	Loss, misuse, or unauthorised access could result in reputational loss and litigation.	Teaching data Governance records
LOW	Loss, misuse, or unauthorised access could result in reputational loss.	Management information Collection's data Public facing content

Legal and Regulatory Obligations

The use of information is governed by a number of different Acts of Parliament.

All users have an obligation to comply with current relevant legislation which includes, but is not limited to:

Computer Misuse Act (1990)

The Data Protection Act (1998)

Freedom of Information Act (2000)

Copyright, Designs and Patents Act (1988)

Regulation of Investigatory Powers Act (2000)

Human Rights Act (2000)

Electronic Communications Act (2000)

Digital Economy Act (2010)

Obscene Publications Act (1959• & 1964)

Counterterrorism and Security Act (2015)

Breaches of Security

Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform their immediate line manager. They will advise on what steps should be taken to avoid incidents or minimize their impact and identify action plans to reduce the likelihood of recurrence.

In the event of a suspected or actual breach of information security, IT Security, with or without consultation with the relevant department, may require that any systems suspected of being compromised are made inaccessible.

Where a breach of security involving either computer or paper records relates to personal information, the Dar Ul Madinah Data Protection Officer must be informed, as there may be an infringement of the Data Protection Act 1998.

All physical security breaches should be reported to the Governor's

Policy Awareness and disciplinary procedure

This policy will be provided to all new and existing staff, students, and members of Dar Ul Madinah. All other users of Dar Ul Madinah's information systems will be advised of the existence of this policy, which will be made available on the Dar Ul Madinah website.

All users are required to familiarise themselves with this policy and comply with its requirements.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action.

Dar Ul Madinah may refer the user to the police where it reasonably believes a crime has been committed and will co-operate fully with any police investigations.

23. INFORMATION TRANSFER OUTSIDE THE EEA

Following an information audit, it was found that no data is currently sent outside the EEA. It is also not envisaged that this will ever be the case.

24. PERSONAL DATA BREACHES

Breaches will be reported to the ICO within 72 hours by both processors and controllers.

All Dar Ul Madinah personnel need to be aware that failure to report will result in a fine.

Only those breaches that could cause harm to data subjects need to be reported, but all breaches will be recorded by Dar Ul Madinah and reported to the governors.