

Nadeen School Data Protection Policy

Nadeen School Data Protection Policy.....	1
Policy Statement.....	2
About this Policy.....	2
Data Protection Officer.....	3
Fair and Lawful Processing.....	4
Special Category Personal Data.....	5
Vital Interests.....	5
Consent.....	6
Processing for Limited Purposes.....	6
Notifying Data Subjects.....	7
Adequate, Relevant and Non-excessive Processing.....	7
Accurate Data.....	7
Timely Processing.....	8
Processing in line with Data Subject's Rights.....	8
The Right of Access to Personal Data.....	8
The Right to Object.....	8
The Right to Rectification.....	9
The Right to Restrict Processing.....	9
The Right to Be Forgotten.....	10
Right to Data Portability.....	11
Data Security.....	11
Personal Data Breach Reporting & Timelines.....	12
Data Protection Impact Assessments.....	13
Disclosure and Sharing of Personal Information.....	13
Data Processors.....	13
Cross-Border Data Transfers and Cloud Services.....	14
Images and Videos.....	14
Categorisation of Image Use and Consent Requirements.....	15
School Event Guidelines for Parents and Students.....	15
Managing Objections.....	16
Biometric Data (Attendance System).....	16
CCTV.....	16
Changes to this Policy.....	16
MEDIA CONSENT FORM.....	17
Taking, Storing and Using Student Images Policy.....	19
ANNEX DEFINITION OF TERMS.....	23
CCTV Policy.....	25
1. Purpose and Lawful Basis.....	25
2. System Scope and Camera Siting.....	25
3. System Access, Governance, and Technical Support.....	25
4. CCTV Access Logs and Audit Trails.....	26
5. Data Storage, Retention, and Export Rules.....	26
6. Subject Access Requests (SARs) and Third-Party Rights.....	27



Policy Statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a school we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

This policy exists in conjunction with Bahrain Law No. 30 of 2018 and with reference to the following school SOP/policies: Acceptable Use Agreement, CCTV Policy, Online safety Policy, Devices- Personal and Work Policy etc.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this Policy

The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in Bahrain's Personal Data Protection Law of 2018 (Law Number 30 of 2018 Issuing the Data Protection Law).

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time. However, adhering to the rules and regulations within Bahrain is contractual.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Definition of Data Protection Terms: All defined terms in this policy are indicated in bold text, and a list of definitions is included in the Annex to this policy.

Data Protection Officer

1.1 As a school we are required to appoint a Data Protection Officer (DPO). Our DPO is Maryam AlMoosawi, and she can be contacted at maryam.almosawi@nadeenschool.com.

1.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

1.3 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

Data Protection Principles

2.1 Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- processed fairly and lawfully and transparently in relation to the data subject
- processed for specified lawful purposes and in a way, which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date not kept for any longer than is necessary for the purpose
- processed securely using appropriate technical and organisational measures.

Personal data must also:

- be processed in line with data subjects' rights
- not be transferred to people or organisations situated in other countries without adequate protection.
- We will comply with these principles in relation to any processing of personal data by the school.

Fair and Lawful Processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed
- why the personal data is being processed

- what the lawful basis is for that processing (see below)
- whether the personal data will be shared, and if so with whom
- the period for which the personal data will be held
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the Personal Data Protection Authority (PDPA) in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. At Nadeen School, we map our core data processing activities to the following lawful bases:

- **Performance of a Contract:** Where processing is necessary to fulfill a contract between us and the data subject. Examples include processing staff employment records, payroll administration, and fulfilling parent enrollment/educational contracts.
- **Legal Obligation:** Where processing is necessary to comply with a legal requirement to which the school is subject. Examples include maintaining attendance tracking, mandatory reporting to the Ministry of Education (MoE), and maintaining safeguarding and child protection (CPOMS) records.
- **Legitimate Interests:** Where processing is necessary for a legitimate reason, provided it does not override the fundamental rights and freedoms of the data subject. Examples include CCTV monitoring for campus security, IT network monitoring, and general school administrative communications.
- **Explicit Consent:** Where none of the above apply, we will seek the clear, explicit consent of the data subject prior to processing their personal data. Examples include the use of photographs or videos for public marketing and social media, or processing biometric data (such as fingerprint scanning).

Special Category Personal Data

When special category personal data (such as health, biometric, or ethnic data) is being processed, an additional legal ground must apply to that processing. We will normally only process special category personal data under the following legal grounds:

- **Employment Law Purposes:** Where necessary for employment obligations, for example, processing staff sickness absence records.

- **Substantial Public Interest:** Where necessary for broader public interests, for example, ensuring equality of opportunity or fulfilling statutory safeguarding requirements.
- **Health or Social Care Purposes:** Where necessary for medical reasons, for example, maintaining records in relation to pupils with medical conditions, severe allergies, or specific educational disabilities.
- **Explicit Consent:** Where none of the above apply, we will seek the explicit, written consent of the data subject to process their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information (such as at the time when a pupil joins us).

If any data user is in doubt as to whether they can use any personal data for any purpose, they must contact the DPO before doing so.

Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

- Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.
- There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.
- When students and/or our workforce join Nadeen School a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, among other things. Where appropriate third parties may also be required to complete a consent form.
- Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.
- The DPO must always be consulted in relation to any consent form before consent is

obtained.

- In relation to all pupils we will seek consent from an individual with parental responsibility for that pupil.
- A record must always be kept of any consent, including how it was obtained and when.
- If consent is required for any other processing of personal data of any data subject then the form of this consent must:
 - inform the data subject of exactly what we intend to do with their personal data
 - require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
 - inform the data subject of how they can withdraw their consent.

Processing for Limited Purposes

In the course of our activities as a school, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our workforce).

We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about:

1.1 our identity and contact details as Data Controller and those of the DPO

1.2 the purpose or purposes and legal basis for which we intend to process that personal data

1.3 the types of third parties, if any, with which we will share or to which we will disclose that personal data

1.4 whether the personal data will be transferred outside Bahrain and if so the safeguards in place

1.5 the period for which their personal data will be stored, by reference to our Retention and Destruction Policy



1.6 the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making

1.7 the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the Bahrain Personal Data Protection Authority (PDPA).

1.8 Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

Accurate Data

We will ensure that personal data we hold is accurate and kept up to date.

We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

Processing in line with Data Subject's Rights

1. We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them

- object to the processing of their personal data, including the right to object to direct marketing
2. Have inaccurate or incomplete personal data about them rectified
- restrict processing of their personal data
 - have personal data we hold about them erased
 - have their personal data transferred
 - object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the school's Subject Access Request Procedure, and Nadeen School will provide a response within the explicit statutory response limits: 15 working days under the Bahrain PDPL, or 1 calendar month under GDPR. If we consider the request to be too complex to resolve within that period, then we may extend the response period by a further 15 days (under PDPL) or two months (under GDPR). If this is necessary, we will inform the data subject within the initial response window that this is the case.

The Right to Object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right. In respect of direct marketing any objection to processing must be complied with.

The school is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

If a data subject informs Nadeen School that personal data held about them by Nadeen School is inaccurate or incomplete, then we will consider that request and provide a response within the explicit statutory response limits: 15 working days under the Bahrain PDPL, or 1 calendar

month under GDPR. If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further 15 days (under PDPL) or two months (under GDPR). If this is necessary, then we will inform the data subject within the initial response window of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances, we will inform the data subject of their right to complain to the Data Protection Authority at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to 'block' or suppress the processing of personal data. This means that Nadeen School can continue to hold the personal data but not do anything else with it.

Nadeen School must restrict the processing of personal data:

- where it is in the process of considering a request for personal data to be rectified (see above)
- where Nadeen School is in the process of considering an objection to processing by a data subject
- where the processing is unlawful, but the data subject has asked Nadeen School not to delete the personal data
- where Nadeen School no longer needs the personal data, but the data subject has asked the school not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the school.

If Nadeen School has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

If a data subject makes a request to have their personal data erased, Nadeen School will consider that request and provide a response within the explicit statutory response limits: 15 working days under the Bahrain PDPL, or 1 calendar month under GDPR. If we consider the issue to be too complex to resolve within that period, then we may extend the response period

by a further 15 days (under PDPL) or two months (under GDPR). If this is necessary, we will inform the data subject within the initial response window that this is the case. Data subjects have a right to have personal data about them held by Nadeen School erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected.
- When a data subject withdraws consent – which will apply only where the school is relying on the individual's consent to the processing in the first place.
- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
- Where the processing of the personal data is otherwise unlawful.
- When it is necessary to erase the personal data to comply with a legal obligation.

Nadeen School is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- to exercise the right of freedom of expression or information
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- for public health purposes in the public interest
- for archiving purposes in the public interest, research or statistical purposes
- in relation to a legal claim.

If Nadeen School has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

Right to Data Portability

In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation.

If such a request is made then the DPO must be consulted.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:

- **Sensitive Data Transfer:** Sensitive data will be transferred and shared between staff through secured/encrypted channels.
- **Entry Controls:** Any stranger seen in entry-controlled areas should be reported to a member of SLT.
- **Secure Lockable Desks and Cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of Disposal:** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Data Protection Authority's guidance on the disposal of IT assets.
- **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended.
- **Working Away from School Premises – Paper Documents:** Paper documents are only to be taken off site if there is no other alternative and with express written consent from management - Executive Leadership Team. The school's code of conduct must be followed at all times. No hard copy documents must be left in vehicles or places other than the home address of the member of staff. Hard copies must be left in a secure place in the home and be returned to school as soon as possible. No copying of the documents must take place. Any breach of security must be notified to the DPO and SLT. Refer to the User Agreement for more details.
- **Working Away from School Premises – Electronic Working:** Staff are only allowed to work from a secure network and downloading of information onto personal devices is prohibited. Access to work emails and other work sites must be password protected and the password must not be shared with anyone else. Portable data devices such as USBs etc may only be used if they have been encrypted. Any existing devices need to be encrypted by IT services. Upon termination of contract staff should delete data from all such devices. Any data breach must be reported immediately to the DPO, SLT and the Head of IT. Refer to the User Agreement for more details.

- **Document Printing:** Documents containing personal data must be collected immediately from printers and not left on photocopiers. Document access and printing are restricted to users with individual, password-protected logins. Users must not share credentials, and all usage is monitored to ensure secure and responsible access.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Personal Data Breach Reporting & Timelines

In the event of a known or suspected personal data breach (including unauthorized access, loss, theft, or exposure of personal data):

- **Internal Escalation:** All workforce members must immediately report suspected security incidents or personal data breaches to the Data Protection Officer (DPO) and IT Helpdesk.
- **Assessment Window:** The DPO, Head of IT, and Senior Leadership Team (SLT) will immediately investigate and conduct a risk assessment of the incident.
- **Regulatory Notification (72-Hour Limit):** For any breach that poses a risk to the rights, privacy, or safety of individuals, Nadeen School will report the incident to the Bahrain Personal Data Protection Authority (PDPA) (and/or relevant supervisory authorities under GDPR where applicable) without undue delay and within 72 hours of becoming aware of the breach.
- **Notification to Affected Individuals:** If the breach is likely to result in a high risk to affected pupils, parents, or workforce members, the school will notify the affected data subjects directly without undue delay, providing actionable advice on protective measures.
- **Breach Logging:** All data breaches and security incidents—regardless of whether they meet the threshold for external reporting—will be recorded in the school’s internal Data Breach Register along with corrective actions taken.

Data Protection Impact Assessments

Nadeen School takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk



to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

The school will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

Disclosure and Sharing of Personal Information

We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Ministry for Education, Bahrain Quality Assurance Authority, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The school will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Data Processors

We contract with various organisations who provide services to the school, including:

Examples include: iSAMs; Classe365; Microsoft; Century Tech; CPOMs; Class Dojo; Google; MoE Database; External Examinations bodies; Insurance providers; Government Relations Officer; National College; GL Assessments; Learning Ladders.

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, sensitive data will be transferred through secured/encrypted channels, or if they put in place adequate measures themselves to the satisfaction of the school. The school will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit

obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

Cross-Border Data Transfers and Cloud Services

To deliver effective administrative, educational, and communication services, the school utilises specialised third-party cloud-based software and platforms (including, but not limited to, iSAMS, Microsoft, Google, Century Tech, CPOMs, and GL Assessments). Certain systems host, back up, or process personal data on secure servers located outside the Kingdom of Bahrain.

Safeguards for Transfers: The school will only transfer or host personal data outside the Kingdom of Bahrain where appropriate transfer safeguards are established in accordance with Bahrain Law No. 30 of 2018 (PDPL) and Ministerial Resolution No. 42 of 2022 regarding cross-border data transfers.

Due Diligence: Prior to transferring data overseas or adopting international cloud platforms, the school conducts strict due diligence to verify that data processors implement adequate technical and organizational security measures, adhere to strict confidentiality duties, and execute binding data processing agreements compliant with Bahrain legal standards.

Images and Videos

General Principles

Images, video, and audio recordings of pupils are used to celebrate student achievements (academic, sporting, and extracurricular), support internal administration, and promote the work of the school. The school ensures that all images are obtained, processed, and stored responsibly in accordance with Bahrain Law No. 30 of 2018 the detailed provisions in [Taking, Storing and Using Student Images Policy](#). Whenever a pupil begins their attendance at Nadeen School they, or their parent, where appropriate, will be asked to complete an [media consent form](#) in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

Categorisation of Image Use and Consent Requirements

In accordance with Section 6 of this policy, consent for image and video use must be freely given on an opt-in basis. To ensure full transparency and give parents granular control, the Photo Consent Form segregates image use into the following specific categories:

- **Identification:** Images stored in the school's Information Management System solely for

student identification, security, and administrative purposes (processed under the school's legitimate administrative duties).

- **Internal Use:** Images displayed within the school premises or on secure internal networks (e.g., hallway wall displays, class projects, School Yearbook, school calendars, exam board submissions, parent web platforms, and internal staff/student presentations).
- **Social Media:** Images shared on Nadeen School Bahrain's official social media platforms (e.g., Facebook, Instagram, LinkedIn, YouTube).
- **Press, Public Relations, & Public Events:** Images shared with newspapers/magazines, in event booklets, or during public community events (e.g., festive fairs, music concerts, school productions).
- **School Marketing & Publications:** Images used on the official school website and in print marketing materials (e.g., prospectuses, brochures, flyers, announcements, school advertising, and press releases).
- **External Mass Media Advertising:** Explicit, additional consent is obtained before any student image or recording is used for external mass media advertising campaigns (e.g., television, radio, commercial billboards, or third-party advertising).
- **Safeguards & Anonymity:** Children's full names will not accompany their photographs on official social media, news, or promotional posts unless explicit parent/guardian consent has been obtained for that specific publication.

School Event Guidelines for Parents and Students

- Parents and guests attending school events may take photographs/videos for personal, domestic use only. They must not post images containing other pupils on public social media.
- Flash photography is strictly forbidden during indoor performances.
- Taking photographs or videos in sensitive areas (restrooms, changing rooms, swimming pools, backstage) is strictly prohibited for both parents and pupils.
- Students must obtain explicit consent from teachers and peers before filming or taking photos.

Managing Objections

Parents or guardians may update their preferences or object to the use of their child's images at any time by contacting the Marketing Department marketing@nadeenschool.com or the Admissions Department admissions@nadeenschool.com depending on the category and amendment required, this amendment will be also reviewed and logged by the School DPO in



accordance with [Taking, Storing and Using Student Images Policy](#).

Biometric Data (Attendance System)

Nadeen School uses a biometric fingerprint system (BioTime) to support staff attendance and payroll processing. Under Data Protection Legislation, biometric data is classified as Special Category Personal Data. Therefore, its use is strictly voluntary and relies on Explicit Consent.

- **Opt-In Process:** Staff will be provided with a standalone, explicit consent form during the HR onboarding process if they wish to use the biometric scanner for their own convenience.
- **Alternatives Provided:** A non-biometric alternative (such as a secure PIN code) will always be made available to any staff member who prefers not to use the fingerprint system. Choosing the alternative method will not negatively impact the employee in any way.
- **Right to Withdraw:** Staff who opt-in may withdraw their consent at any time by notifying HR and the IT Department, at which point their biometric data will be permanently deleted from the system and they will be transitioned to the alternative sign-in method.

CCTV

Nadeen School operates a CCTV system. Please refer to the school's [CCTV Policy](#).

Changes to this Policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

MEDIA CONSENT FORM

Throughout your child's time at Nadeen School, photographs, videos, and audio recordings may be taken to support learning, celebrate achievements, document school life, and communicate with our community.

We take the privacy of our learners seriously and manage all images in accordance with our [Taking, Storing and Using Student Images Policy](#) and the Kingdom of Bahrain's Personal Data Protection Law (PDPL).

Essential Internal & Operational Processing (Legitimate Interest)

The School processes student photographs based on our legitimate interests and legal safeguarding obligations. This processing is strictly limited to essential internal, administrative, security, and health and safety functions, such as profile pictures on the Management



Information System (MIS), safeguarding registers, medical/allergy identification charts, and security CCTV. **As these images are required for routine operational and safety purposes, separate parental consent is not required. These internal photographs will never be published externally or used in public-facing or school community materials (such as yearbooks, newsletters, or social media). Consequently, these core processing activities apply irrespective of your consent selections or opt-out status below.**

Examples of internal operational processing include:

- Student identification profile photos within the Management Information System (MIS)
- Internal safeguarding records and emergency contact registers
- Medical, dietary, and allergy identification charts for staff awareness and student safety
- Campus security and CCTV records
- Celebratory images and videos for our internal community newsletter.

Optional Marketing, Social Media & Community Communications

From time to time, we would like to celebrate our learners and communicate school activities with our community or promote the School externally.

These uses are entirely optional and will ONLY take place if you provide your explicit consent below:

- School website and official public social media (Facebook, Instagram, LinkedIn, YouTube)
- School yearbooks, newsletters, and community event programmes
- Prospectuses, brochures, print advertisements, and press releases

Consent for the Use of Student Images

Please review the options below. You will be required to select **OPT-IN** on the **Application Form** to give your explicit consent for each category:

1. General School & Community Communications

Action Required on Application Form: Please select OPT-IN on the application form if you give permission for Nadeen School Bahrain to use photographs, videos, and/or audio recordings of your child for school community communications and celebrations. This includes parent communications, the school yearbook, internal display boards, event programmes, and password-protected parent portals.

If you do not explicitly opt in on the application form, the School will record this as an



opt-out. Your child's image will not be used in yearbooks, external newsletters, websites, social media, or any school open community communications.

2. External Marketing, Social Media & Public Relations

Action Required on Application Form: Please select OPT-IN on the application form if you give permission for Nadeen School Bahrain to use photographs, videos, and/or audio recordings of your child for external marketing, promotional campaigns, public relations, official public social media platforms (such as Instagram, Facebook, LinkedIn, YouTube), website promotional media, and print advertising.

If you do not explicitly opt in on the application form, the School will record this as an opt-out. Your child's image will not be used for any external marketing, public social media, or promotional materials.

Updating Preferences: If you wish to change your preferences at any time, please contact the Marketing Department at marketing@nadeenschool.com or the admissions team at admissions@nadeenschool.com. We will process your request in accordance with the Personal Data Protection Law (PDPL) and within the applicable statutory timeframes.

Declaration & Acknowledgment

By completing the Application Form, you acknowledge that you have read and understood how student images, video, and audio are managed by Nadeen School Bahrain. Your selections on the Application Form will remain active for the duration of your child's enrolment unless you submit an update to the Marketing or Admissions teams.

Taking, Storing and Using Student Images Policy

1 Introduction

Nadeen School Bahrain (hereafter referred to as "the School") respects your right to data privacy. This Policy is intended to provide information to learners and their parents, carers or guardians (hereafter referred to as "parents") about how images of learners are normally used by Nadeen school Bahrain (hereafter referred to as "the School").

This policy also covers the School's approach to the use of cameras and filming equipment at School events and on School premises by parents and learners themselves.

2 Overview

During the course of the year, photographs, video and/or audio recordings (hereafter referred to as 'images' or 'recordings') of your child(ren) will be taken.

Certain uses of images are necessary for the ordinary running of the School; other uses are in the legitimate interests of the School and its community. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

We hope parents will feel able to support the School in using student images to celebrate the achievements of learners (eg. sporting, academic, extracurricular, etc); to promote the work of the School; and for important administrative purposes such as identification and security.

3 How images / recordings are obtained

3.1 School staff

Images or recordings of learners may be taken by authorised / relevant members of staff (eg. Marketing Department, relevant teachers / admin staff etc).

All staff are given guidance on the School's Policy on Taking, Storing and Using Images of Students, and on the importance of ensuring that images of learners are made and used responsibly, only for school purposes, and in accordance with School policies and the law.

3.2 Professional agencies, photographers, videographers / media and press

Occasionally, the School may invite professional agencies, photographers, videographers or members of the media / press to the School to take photographs or videos (eg. School-wide photos, School events, etc).

Professional photographers and the media are accompanied at all times by a member of staff when on school premises. The School uses only reputable professional photographers/media outlets and makes every effort to ensure that any images of learners are held by them securely, responsibly, and in accordance with the School's instructions.

3.2.1 Data Retention and Storage

All captured photos and video footage must be synced directly to the designated School shared drive to which the photographer or media outlet has been granted access. Furthermore, all local copies must be permanently deleted from capture devices (such as camera memory cards)

within 7 days of the shoot, and from any external editing tools, local drives, or storage locations owned by the agency within 2 weeks of completion.

4 Types of image / recording use

Unless a parent has requested otherwise, the School will use images / recordings of its learners for the following purposes:

- **Identification:** An image of each student is kept in the School's Information Management System for identification purposes.
- **Internal:** Student images may be displayed internally / on School networks (eg. School Yearbook, class / hallway wall displays, School calendars, class projects, exam board submissions, parent web platforms, staff / student presentations, etc);
- **Social media:** Student images may be shared on Facebook, Instagram, LinkedIn, YouTube and any other social media platforms used by Nadeen School Bahrain;
- **Press, public relations, public events:** Student images may be shared with newspapers / magazines, or in booklets / participation at public events (eg. festive fair, music events, productions, etc);
- **Marketing and communications:** Student images and recordings will only be used in the School's marketing, communications, and promotional materials where a parent or legal guardian has explicitly opted in through the application at the time after reviewing the [Media Consent Form](#). Such materials may include, but are not limited to, the School website, social media platforms, prospectuses, brochures, newsletters, flyers, advertisements, billboards, press releases, event programmes, and other printed or digital publications.

5 How we store images and security of access

The School takes appropriate technical and organisational security measures to ensure that images of learners held by the School are kept securely and protected from loss or misuse.

Images and recordings of learners are stored securely within the School's approved systems, including the School's Google Workspace for Education environment (Google Drive) and the School Management Information System (MIS). Access to these systems is restricted to authorised staff members whose roles require such access. Encrypted offline backups may also be maintained for business continuity and disaster recovery purposes.



The School retains images and recordings only for as long as necessary for the purposes for which they were collected and in accordance with the School's Data Protection Policy and applicable data retention requirements.

Routine images and recordings, including those used for day-to-day school communications, marketing and operational purposes, will be retained for 10 years for as long as they remain relevant to those purposes.

Archive-worthy images and recordings, which document the history, heritage, significant milestones or achievements of the School, may be retained indefinitely as part of the School's historical archive. Such images will be securely stored and used only for appropriate educational, historical or institutional purposes. This will have limited access to the Head of IT and Head of Marketing.

6 Objections to image use

Nadeen School Bahrain respects the right of parents to object to their child's images being used in publicity and marketing materials.

Any parent who wishes to limit or object to the use of images of their child should contact the School's Marketing Department. Any requests sent to the Marketing Department should be formally logged with the DPO so that data subject rights (e.g., restriction, erasure, objection) are consistently managed.

The Marketing Department will process the parent's request in accordance with the Personal Data Protection Law (PDPL) and within the applicable statutory timeframes. Where appropriate, the School will take reasonable steps to implement the requested changes and will confirm the action taken. If the School is unable to comply with all or part of the request, it will explain the reasons, including any legal, practical or technical limitations.

7 Limitation of liability

As stated in this policy, the School may share images of learners on its official social media platforms or other marketing channels. Nadeen school Bahrain shall not be held liable for any misuse or misappropriation of these images by third parties.

8 Photography and Filming by Parents and Attendees at School Events



We understand that parents and carers enjoy capturing special school moments and are welcome to take photographs or short videos of their own child during school events, in line with the Parent Code of Conduct and the guidelines below:

- **Event Courtesy:** Please be considerate of other families, students, and performers when using cameras or mobile devices. At indoor events such as assemblies, concerts, or productions, **flash photography must not be used**, as it can distract performers, disturb the audience, and affect individuals with specific medical conditions.
 - **Focusing on Your Child:** Parents should avoid taking photographs or videos of other students, except where they appear incidentally in a wider group image.
 - **Personal & Private Use Only:** Any photographs or videos taken at school events are for personal and private use only. Images or recordings that identify other students **must not be shared on social media, messaging platforms, websites, or any other public forum** without appropriate consent from those students' families.
 - **Copyright Restrictions:** In some cases, copyright restrictions may prevent photography or filming during specific performances. Where this applies, the School will notify parents in advance and request that these requirements are respected.
-
- **Strictly Prohibited Areas:** Photography and filming are **strictly prohibited** in areas where privacy is expected, including changing rooms, backstage areas, or swimming pool facilities when children may be in a state of undress.
 - **Respecting Privacy Requests:** If any student, parent, or member of staff expresses concern about being photographed or filmed, we ask that their wishes are respected immediately.

The School reserves the right to restrict or withdraw permission to take photographs or videos at any time if these guidelines are not followed or if photography/filming is deemed inappropriate.

Thank you for helping us celebrate our students' achievements while respecting the privacy, dignity, and safety of every member of our school community.

ANNEX DEFINITION OF TERMS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a Bahraini national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Those of our workforce (including volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Term	Definition
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes any individual employed by Nadeen School such as staff and those who volunteer in any capacity including trustees / members/ parent helpers.

CCTV Policy

1. Purpose and Lawful Basis

Nadeen School operates a Closed-Circuit Television (CCTV) system across its campus to maintain a safe and secure environment for pupils, staff, and visitors, protect school property, and assist in preventing or investigating incidents.



This processing is conducted under the school's **Legitimate Interests** and statutory duty of care to maintain campus security under Bahrain's Personal Data Protection Law (PDPL).

2. System Scope and Camera Siting

- Cameras are positioned strategically at campus entry/exit points, perimeter fences, outdoor grounds, and key indoor common areas (such as corridors and shared facilities).
- Cameras are **never** placed in private locations, including changing rooms, restrooms, or staff private areas.
- **Audio Prohibition:** In compliance with PDPL principles, audio recording features on all campus CCTV cameras are strictly disabled.
- Clear signage is prominently displayed throughout the school to inform individuals that CCTV monitoring is in operation.

3. System Access, Governance, and Technical Support

- **Authorised System Managers:** Full administrative access to CCTV systems is restricted to the Principal, Vice Principal, Health & Safety Officer, Safeguarding Team, and Data Protection Officer (DPO).
- **Security Team Duties:** Security Guards on duty are permitted to monitor **live feeds** purely for real-time campus safety. Security Guards are strictly prohibited from accessing or reviewing recorded historical footage unless explicitly authorized by the Health & Safety Officer, Principal, or Safeguarding Lead.
- **Staff Incident Investigations:** Teachers and staff members may view specific recorded footage to investigate student discipline, safety breaches, or safeguarding incidents, provided the viewing is monitored by an Authorised System Manager and pre-approved by the Principal, Safeguarding Lead, Health & Safety Officer, or DPO.
- **Technical Infrastructure & Third-Party Vendors:** The IT Department, alongside our contracted external network vendor operating under an **Annual Maintenance Contract (AMC)**, provides technical infrastructure support (network management, server maintenance, account provisioning, and firmware configurations for retention loops and audio disabling). All external vendors are bound by Data Processing Agreements (DPAs) under the PDPL. Neither internal IT staff nor external vendor engineers are authorised to view or review CCTV footage unless explicitly requested to provide technical assistance under the direct supervision of an Authorised System Manager or the DPO.

4. CCTV Access Logs and Audit Trails

- The Security Team maintains a daily **CCTV Access Logbook** recording every instance where recorded footage is viewed or reviewed.
- The log records the date, time, camera location, reason for viewing, guard/staff name, and the name of the approving manager.
- The Health & Safety Officer conducts routine reviews of the logbook, and the log remains subject to periodic compliance audits by the DPO.

5. Data Storage, Retention, and Export Rules

- **Retention Period:** Standard CCTV footage is recorded continuously and retained securely on encrypted local servers for a maximum of **120 days**. On day 121, older recordings are automatically deleted and overwritten by the system, unless specific footage has been saved and retained for an ongoing investigation, Subject Access Request (SAR), or legal claim.
- **Internal Exports:** Exporting or saving video clips for internal school investigations is restricted and requires written approval from the Principal or Health & Safety Officer. Exported files must be stored on secure, encrypted school storage and permanently deleted once the investigation concludes.
- **External Disclosures:** Footage files will **never** be exported or released to external third parties (including parents, law enforcement, or regulatory authorities) without prior review and written clearance from the **Data Protection Officer (DPO)** to ensure third-party face blurring (redaction) and legal compliance under the PDPL when possible.
- **Prohibited Recording:** Mobile phone recordings, screen captures, or unofficial downloads of CCTV displays by staff are strictly prohibited and constitute a disciplinary offense.

6. Subject Access Requests (SARs) and Third-Party Rights

- Individuals (or parents/guardians acting on behalf of pupils) have the right to request access to CCTV footage containing their own personal data by submitting a formal Subject Access Request (SAR) via email to the Principal, Vice Principal, Health & Safety Officer, or DPO (maryam.almosawi@nadeenschool.com).



- **Third-Party Privacy Protection:** Before any CCTV footage is disclosed to a requester, all third-party identifying features (such as the faces of other pupils, staff, or visitors) must be pixelated or blurred under DPO supervision. If redaction is technically unfeasible, the school reserves the right to refuse footage disclosure and provide a descriptive written summary instead.