

Newton International Academy, Barwa

Data Proctection Policy

An International Community of Learners, Striving for Excellence and Celebrating Success

Approved by: Senoir Management Team
Date Approved: September 2026
Next Review Date: September 2027
Review Cycle: Annual

NEWTON INTERNATIONAL ACADEMY | BARWA

Statement of Intent

Newton International Academy Barwa (NIA) is committed to safeguarding the personal data of its staff members and students. This policy ensures compliance with the General Data Protection Regulation (GDPR) and relevant local laws, thereby fostering a culture of transparency and accountability in data management. NIA recognises the importance of protecting personal information and is dedicated to maintaining the highest standards of data protection.

Vision

An international community of learners striving for excellence and celebrating success.

Mission

We aim to provide the highest quality of education possible for our students of all abilities. In doing so, we aim to positively encourage each student to achieve academic excellence, enjoy creative diversity, develop critical thinking skills, and become lifelong learners and responsible citizens.

To achieve this, we will provide a diverse education in a safe, supportive environment that promotes self-discipline and motivation. We will provide and maintain a calm, trusting, and caring atmosphere where teaching and learning are meaningful and developed. We will work in partnership with our staff, students, parents, and the wider community to achieve our vision.

Rationale

In an increasingly digital world, the protection of personal data is paramount. NIA is committed to ensuring that all data processing activities are conducted in compliance with GDPR and relevant local laws, thereby safeguarding the rights and freedoms of individuals. This policy outlines the principles and practises that guide our data protection efforts, ensuring that all stakeholders understand their responsibilities in managing personal data.

Aim

The aim of this policy is to outline how NIA manages personal data in compliance with GDPR and other relevant legislation. It sets forth the principles of data protection, the rights of individuals, and the responsibilities of staff in handling personal data.

Newton Group Values:



1. Legal Framework

This policy is established in accordance with the following legislation:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

2. Applicable Data

2.1 Personal Data: Refers to any information that relates to an identifiable, living individual, including names, contact details, and online identifiers.

2.2 Sensitive Personal Data: Includes special categories of personal data as defined by GDPR, such as genetic data, biometric data, and health-related information.

3. Principles

In accordance with GDPR, personal data will be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up-to-date.
- Retained for no longer than necessary.
- Processed securely to protect against unauthorised access, loss, or damage.

4. Accountability

NIA will implement measures to demonstrate compliance with data protection principles, including:

- Clear and transparent privacy policies.
- Internal records of processing activities.
- Regular audits and assessments of data protection practices.

5. Data Protection Officer (DPO)

5.1 A DPO will be appointed to oversee compliance with GDPR and provide guidance on data protection matters.

5.2 The DPO will have professional expertise in data protection law and report directly to the Principal.

6. Lawful Processing

6.1 Data will be processed lawfully under conditions such as consent, legal obligation, public interest, and legitimate interests.

6.2 Sensitive data will only be processed under specific conditions outlined in GDPR.

7. Consent

7.1 Consent will be sought where necessary and must be clear, informed, and freely given.

7.2 Individuals can withdraw consent at any time, and mechanisms for obtaining consent will comply with GDPR standards.

8. The Right to Be Informed

8.1 Individuals will be provided with clear information regarding the processing of their personal data, including the purpose of processing and their rights.

9. The Right of Access

9.1 Individuals have the right to access their personal data and request confirmation of its processing.

10. The Right to Rectification

10.1 Individuals can request correction of inaccurate or incomplete personal data.

11. The Right to Erasure

11.1 Individuals have the right to request deletion of their personal data under certain conditions.

12. The Right to Restrict Processing

12.1 Individuals can request restriction of their personal data processing under specified circumstances.

13. The Right to Data Portability

13.1 Individuals have the right to obtain and reuse their personal data across different services.

14. The Right to Object

14.1 Individuals can object to the processing of their personal data in certain situations.

15. Automated Decision Making and Profiling

15.1 NIA will ensure that individuals are not subject to decisions based solely on automated processing unless specific conditions are met.

16. Privacy by Design and Privacy Impact Assessments

16.1 NIA will implement data protection measures from the outset of any data processing activity and conduct privacy impact assessments where appropriate.

17. Data Breaches

17.1 NIA will have procedures in place to detect, report, and investigate personal data breaches.

18. Data Security

18.1 NIA will implement appropriate technical and organisational measures to ensure the security of personal data.

19. Publication of Information

19.1 NIA will ensure that information about its data processing activities is publicly available and accessible.

20. CCTV and Photography

20.1 The use of CCTV and photography will be conducted in compliance with data protection regulations, ensuring transparency and respect for individual privacy.

21. Data Retention

21.1 Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected.

22. DBS Data

22.1 Data obtained through the Disclosure and Barring Service (DBS) will be handled in accordance with relevant legislation and guidelines.

23. Policy Review

23.1 This policy will be reviewed annually to ensure it remains compliant with current legislation and best practises.

Key Responsibilities of the Data Protection Officer

1. **Understanding Data Protection Legislation:**
   - The DPO should have a thorough understanding of the UK GDPR, Data Protection Act 2018, and other relevant data protection laws.
   - They should stay updated on changes in legislation and best practises in data protection.
2. **Advising on Compliance:**
   - Provide guidance to the school's leadership and staff on compliance with data protection laws.
   - Assist in the development and implementation of data protection policies and procedures.
3. **Monitoring Data Processing Activities:**
   - Oversee the school's data processing activities to ensure they comply with legal requirements.
   - Conduct regular audits and assessments of data processing operations.
4. **Risk Assessment and Management:**
   - Identify and assess risks related to data processing activities.
   - Recommend measures to mitigate risks and protect personal data.
5. **Training and Awareness:**
   - Participate in and recommend training programmes (such as Data protection on National College) for staff on data protection principles and practises.
   - Foster a culture of data protection awareness within the school community.
   - For DPO - Professional certification in data protection (e.g., CIPP/E, CIPM, or equivalent) is desirable.
6. **Handling Data Subject Requests:**
   - Manage requests from individuals regarding their personal data, such as access requests, rectification, erasure, and data portability.
   - Ensure that responses to these requests are timely and compliant with legal requirements.
7. **Liaising with Regulatory Authorities:**
   - Act as the main point of contact between the school and the Information Commissioner's Office (ICO) or other relevant regulatory bodies.
   - Report any data breaches to the ICO and manage the response to such incidents.
8. **Maintaining Records of Processing Activities:**
   - Keep detailed records of all data processing activities carried out by the school, including the purposes of processing, categories of data, and retention periods.

9. Ensuring Data Security:

- Work with IT and security teams to ensure that appropriate technical and organisational measures are in place to protect personal data.
- Monitor compliance with data security policies and procedures.

Knowledge Areas for the Data Protection Officer

1. Data Protection Laws and Regulations:

- In-depth knowledge of UK GDPR, Data Protection Act 2018, and related legislation.

2. Data Processing Practises:

- Understanding of how personal data is collected, processed, stored, and shared within the school.

3. Risk Management:

- Familiarity with risk assessment methodologies and data protection impact assessments. Remind staff to change their passwords regularly. Manage staff sand student email accounts (students utilising these for online platforms and Unifrog). Ensuring that EO oversees the security of online Exam results.

4. Information Security:

- Knowledge of data security measures and best practises to protect personal data.
- Ensuring the school Intranet, Shared drives, school emails and RENWEB, MyConcern, Blue sky and other software utilised by the school are safe.

5. Training and Communication:

- Skills in developing training materials and communicating data protection principles effectively to staff and stakeholders.

6.Incident Management:

Understanding of procedures for managing data breaches and reporting requirements.

Data Protection Policy

Contents: Statement of intent

- 1. Legal framework
- 2. Applicable data
- 3. Principles
- 4. Accountability
- 5. Data protection officer (DPO)
- 6. Lawful processing
- 7. Consent
- 8. The right to be informe
- 9. The right of access
- 10. The right to rectification
- 11. The rightto erasure
- 12. The right to restrict processing
- 13. The right to data portability

- 14. The right to object
- 15. Automated decision making and profiling
- 16. Privacy by design and privacy impact assessments
- 17. Data breaches
- 18. Data security
- 19. Publication of information
- 20. CCTV and photography
- 21. Data retention
- 22. DBS data
- 23. Policy review

1.Statement of intent

- Newton International Academy (NIA) is accredited by the Department for Education in the UK and as such must comply with all educational standards and laws set.
- NIA is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the General Data Protection Regulation (GDPR). NIA may, from time to time, be required to share personal information about staff or students with other organisations, mainly the DfE, Ministryof Education in Qatar, other schools. This policy is in place to ensure all staff, students and parents are aware of their responsibilities and comply with the following core principles of the GDPR. Organisational methodsfor keeping data secure are imperative, and NIA believes that it is good practice to keep clear practical policies, backed up by written procedures.
- This policy complies with the requirements set out in the GDPR, came into effect on 25 May 2018. The UK Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

- <u>This policy has due regard to legislation, including, but not limitedto the following</u>:

- The General Data Protection Regulation (GDPR) The Freedom of Information Act 2000 The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) The Freedomof Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The School Standards and Framework Act 1998 1.2. This policy will also have regard to the following guidance: InformationCommissioner's Office (2017) 'Overviewof the General Data ProtectionRegulation (GDPR)'Information Commissioner's Office(2017) 'Preparing for the General Data Protection Regulation (GDPR)12 steps to take now' 1.3. This policy will be implemented in conjunction with the following other policies and procedures: ICT Policy E-SafetyPolicy and Acceptable Use Agreement Data Security Breach Prevention and Management Plan Trust Records Retention Schedule

2. Applicable data

2.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be: Processed lawfully, fairly and in a transparent manner in relation to individuals. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. 2 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. Processed in a manner that ensures appropriate security of the personal
data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. NIA will implement appropriate technical and organisational measures to demonstrate that data is processedin line with the principles set out in the GDPR.

4.2. NIA will provide comprehensive, clear and transparent privacy policies.

4.3. Internal records of processing activities will include the following: Name and details of the organisation Purpose(s) of the processing Description of the categories of individuals and personal data Retention schedules Categories of recipients of personal data Description of technical and organisational security measuresDetails of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.4. NIA will implement measures, where appropriate, that meet the principles of data protection by design and data protection by default, such as: Data minimisation. Pseudonymisation. Transparency. Allowing individuals to monitor processing. 3 Continuously creating and improving security features.
4.5. Data protection impact assessments will be used, where appropriate.

5. Data Protection Officer (DPO)

5.1. A DPO will be appointed in order to: Inform and advise NIA and their employees about obligations to comply with the GDPR and other data protection laws. Monitor NIAs' compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments and conducting internal audits.
5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
5.4. The DPO will report to the highest level of management of NIA, namely the Principal.
5.5. The DPO will operate independently and will not be dismissedor penalised for performing their task.
5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.
6.2. Each Newton Group school will act as a data processor; however, third parties may also undertake this role.
6.3. Under the GDPR, data will be lawfully processed under the following conditions: The consent of the data subject has been obtained. Processing is necessary for: Compliance with a legal obligation. The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. For the performance of a contract with the data subject or to take steps to enter into a contract. Protecting the vital interests of a data subject or another person. For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by schools in the performance of their tasks.)
6.4. Sensitive data will only be processed under the following conditions: 4 Explicit consent of the data subject, unless reliance on consent is prohibited by the MoE. Processing relates to personal data manifestly made public by the data subject. Processing is necessary for: Carrying out obligations under employment, social security or social protection law, or a collective agreement. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.The establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity.

Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards. — The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional. — Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices. — Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1.Consent will be sought prior to processing any data whichcannot be done so under any other lawful basis, such as complying with a regulatory requirement.
7.2. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
7.3. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
7.4. Where consent is given, a record will be kept documenting how and when consent was given.
7.5. NIA will ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
7.6. Consentaccepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
7.7. Consent can be withdrawn by the individual at any time.
7.8. Where a child is under the age of 16, or 19 if continuing into 6th Form, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.
7.9. When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consentwill only be gained from students where it is deemed that the pupil has a sound understanding of what they are consenting to.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.
8.2. If services are offered directly to a child, NIA will ensure that the privacy notice is written in a clear, plain manner that the child will understand.
8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject the following information will be supplied within the privacy notice: The contact details of the controller, and where applicable, the controller's representative, as well as the DPO. The purpose of, and the legal basis for, processing the data. The legitimate interests of the controller or third party.

Any recipient or categories of recipients of the personal data. Details of transfers to third countries and the safeguards in place. The retention period of criteria used to determine the retention period. The existence of the data subject's rights, including the right to:
Withdraw consent at any time. Lodge a complaint with a supervisory authority. The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
8.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
8.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Newton Group of schools hold, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied: Within one month of having obtained the data. 6 If disclosure to another recipient is envisaged, at the latest, before the data are disclosed. If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed. 9.2. Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
9.3. NIA will verify the identity of the person making the request before any information is supplied.
9.4. A copy of the information will be supplied to the individual free of charge; however, a 'reasonable fee' may be charged to comply with requests for further copies of the same information.
9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
9.7.All fees will be based on the administrative cost of providing the information.
9.8. All requests will be responded to without delay and at the latest, within one month of receipt.
9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
9.10. Where a request is manifestly unfounded or excessive, NIA holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, NIA will ask the individual to specify the information the request is in relation to.

10. The rightto rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personaldata rectified.

10.2. Where the personal data in question has been disclosed to third parties, NIA will inform them of the rectification where possible.

10.3. Where appropriate, NIA will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, NIA will explainthe reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances: Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed When the individual withdraws their consent When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing The personal data was unlawfully processed The personal data is required to be erased in order to comply with a legal obligation The personal data is processed in relation to the offer of information society services to a child

11.3. NIA have the right to refuse a request for erasure where the personal data is being processed for the following reasons: To exercise the right of freedom of expression and information To comply with a legal obligation for the performance of a public interest task or exercise of official authority For public health purposes in the public interestFor archiving purposes in the public interest, scientific research, historical research or statistical purposes The exercise or defense of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. 11.6. Where personal data has been made public within an online environment, NIA will inform other organisations who process the personal data to erase links to and copies of the personal data in question

12. The right to restrictprocessing

12.1. Individuals have the right to blockor suppress the Newton Group of schools processing of personal data.

12.2. In the event that processing is restricted, NIA will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
12.3. NIA will restrict the processing of personal data in the following circumstances: Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual Where processing is unlawful and the individual opposes erasure and requests restriction instead Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
12.4. If the personal data in question has been disclosed to third parties, NIA will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
12.5. NIA will inform individuals when a restriction on processing has been lifted.

13. The rightto data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
13.3. The right to data portability only applies in the following cases:To personal data that an individual has provided to a controller Where the processing is basedon the individual's consent or for the performance of a contract When processing is carried out by automated means
13.4. Personaldata will be provided in a structured, commonly used and machine- readable form.
13.5. NIA will provide the information free of charge.
13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
13.7. NIA are not required to adopt or maintain processing systems that are technically compatible with other organisations.
13.8. In the event that the personal data concerns more than one individual, NIA will consider whether providing the information would prejudice the rights of any other individual.
13.9. NIA will respond to any requests for portability within one month.
13.10. Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. 13.11. Where no action is being taken in response to a request,NIA will, withoutdelay and at the latestwithin one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. NIA will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the

attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following: Processing based on legitimate interests or the performance of a task in the public interest Direct marketing Processing for purposes of scientific or historical research and statistics. 14.3. Where personal data is processed for the performance of a legal task or legitimate interests: An individual's grounds for objecting must relate to his or her particular situation. NIA will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual. 14.4. Where personal data is processed for direct marketing purposes: NIA will stop processing personal data for direct marketing purposes as soon as an objection is received. NIA cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes. 14.5. Where personal data is processed for research purposes: The individual must have grounds relating to their particular situation in order to exercise their right to object. 10 Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data. 14.6. Where the processing activity is outlined above, but is carried out online, NIA will offer a method for individuals to object online.

15. Automated decisionmaking and profiling

15.1. Individuals have the right not to be subject to a decision when: It is based on automated processing, e.g. profiling. It produces a legal effect or a similarly significant effect on the individual. 15.2.NIA will take steps to ensure that individuals are able to obtain human intervention, express their pointof view, and obtain an explanation of the decision and challenge it. 15.3. When automatically processing personal data for profiling purposes, NIA will ensure that the appropriate safeguards are in place, including: Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact. Using appropriate mathematical or statistical procedures. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects. 15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless: The school has the explicit consent of the individual. The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. Privacy by design and privacy impact assessments

16.1.NIA will act in accordance with the GDPR by adopting 'privacy by design' approach and implementing technical and organizational measures that demonstrate how the school has considered and integrated data protection into processing activities. 16.2. Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with NIA's data protection obligations and meeting individuals' expectations of privacy.

16.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the reputation of NIA.
16.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
16.5. A DPIA will be used for more than one project, where necessary. 16.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences The use of CCTV (Closed Circuit Television).

16.7. The school will ensure that all DPIAs include the following information: A description of the processing operations and the purposes An assessment of the necessity and proportionality of the processing in relation to the purpose An outline of the risks to individuals The measures implemented in order to address risk
16.8. Where a DPIA indicates high-risk data processing, NIA will consult the DPO to seek its opinion as to whether the processing operation complies with the GDPR.

17. Data breaches

17.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
17.2. Service Managers (IT, SIMS, VLE etc) and the Data Protection Coordinator for NIA will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevantsupervisory authority will be informed.
17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becomingaware of it.
17.5. The risk of the breach havinga detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
17.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.
17.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
17.10. Within a breach notification, the following information will be outlined: The nature of the personal data breach, including the categories and approximate number of individuals and records concerned The name and contact details of the DPO An explanation of the likelyconsequences of the personal data breach A description of the proposed measures to be taken to deal with the personal data breach Where appropriate, a description of the measures taken to mitigate any possible adverse effects 17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. Data security

18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

18.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

18.5. Memory sticks will not be used to hold personal information unless they are password protected and fully encrypted.

18.6. All electronic devices are password-protected to protect the information on the device in case of theft, including personal phones if they are used to access work emails.

18.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8. Staff will not use school laptops for personal use.

18.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password. Staff must log off each time when they leave the room they were working in.

18.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

18.11. Circular emails to parents are sent Blind carbon copy (Bcc), so email addresses are not disclosed to other recipients.

18.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow 13 the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

18.14. Before sharing data, all staff members will ensure: They are allowed to share it. That adequate security is in place to protect it. Who will receive the data has been outlined in a privacy notice.

18.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are to be supervised at all times.

18.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.17. NIA takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.18 Services Managers and the Data Protection Coordinator at NIA are responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Publication of information

19.1. NIA publish information that will be made routinely available, including: Policies, procedures and minutes of meetings

19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3. NIA will not publish any personal information, including photos, on their websites without the permission of the affected individual.

19.4. When uploading information to websites, staff are considerate of any metadata.

20. CCTV and photography

20.1. NIA understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. 20.2. NIA notify all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

20.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.4. All CCTV footage will be kept securely, only SLT with the Security Manager are responsible for keeping the records secure and allowing access.

20.5. NIA will always indicate their intentions for taking photographs of students and will retrieve permission before publishing them.

20.6. If the school wishes to use images/video footage of students in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

20.7. Consent is checked and precautions, in line with the E-Safety Policy, are taken when publishing photographs of students, in print, video or on NIAs' websites.

20.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR

21. Data retention

21.1. Data will not be kept for longer than is necessary in accordance with the TrustRecords Retention Schedule.

21.2. Unrequired data will be deleted as soon as practicable.

21.3. Some educational records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

21.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22. DBS data

22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

22.2. Data provided by the DBS will never be duplicated.

22.3. Any third parties who access information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

23. Policy review

23.1. This policy is reviewed annually by the DPO and SMT. The next scheduled review date for this policy is June 2023.

Data Breach Detection, Reporting and Investigation Procedure

1. Purpose

Newton International Academy Barwa (NIA Barwa) is committed to protecting the personal data of students, staff, parents, governors, contractors and visitors. This procedure outlines the steps to detect, report, investigate and respond to actual or suspected data breaches in accordance with GDPR, Data Protection Act 2018, and applicable local legislation.

2. Definition of a Data Breach

A data breach is any incident that results in the accidental or unlawful:

- Loss of personal data
- Destruction of personal data
- Alteration of personal data
- Unauthorized disclosure of personal data
- Unauthorized access to personal data

Examples include:

- Sending confidential information to the wrong recipient
- Lost or stolen laptop, tablet, USB drive or mobile phone
- Sharing student information without authorization
- Emailing parents without using BCC
- Accessing records without a legitimate reason
- Hacking, phishing or malware attacks
- Loss of paper records containing personal information
- Disclosure of examination information to unauthorized persons

3. Immediate Detection and Containment

Any member of staff who discovers or suspects a data breach must:

Step 1 – Act Immediately

Where possible:

- Retrieve the information
- Recall emails
- Secure affected systems
- Change passwords
- Disconnect compromised devices from the network
- Recover paper records if possible

Step 2 – Preserve Evidence

Staff must not:

- Delete emails
- Alter records
- Attempt to hide the incident
- Conduct their own investigation

All evidence must be preserved for investigation.

4. Reporting a Data Breach

Reporting Timeframe

All suspected or confirmed breaches must be reported immediately and no later than:

One hour from discovery

Reporting Route

The staff member must report directly to:

- Data Protection Officer (DPO)
- Principal
- Deputy Principal
- EO/IT Manager (where technology is involved)

Information Required

The report should include:

- Date and time of incident
- Date and time discovered
- Name of person reporting
- Description of incident
- Type of data involved
- Number of individuals affected
- Immediate actions already taken
- Whether data has been recovered

5. Initial Assessment

The DPO will conduct an initial assessment within 24 hours.

The following will be determined:

Risk Level

Low Risk

Examples:

- Email sent internally and immediately deleted
- No sensitive information exposed

Medium Risk

Examples:

- Parent contact information disclosed
- Limited access by unauthorised individual

High Risk

Examples:

- Safeguarding records exposed
- Medical information disclosed
- Student data published online
- Financial information compromised

6. Formal Investigation

The DPO will establish a Data Breach Investigation Team which may include:

- Principal
- Deputy Principal
- IT Manager
- HR Manager
- Relevant Head of School
- Safeguarding Lead (where applicable)

The investigation will determine:

A. What Happened?

- Nature of the breach
- Timeline of events

B. What Data Was Involved?

- Student records
- Staff records
- Parent information
- Medical information
- Examination records
- Safeguarding information

C. Who Was Affected?

- Number of individuals affected
- Categories of affected individuals

D. Cause Analysis

- Human error
- Lack of training
- System failure
- Cyber attack
- Policy non-compliance
- Third-party failure

7. Notification Requirements

Notification to Senior Leadership

The Principal must be informed immediately of all medium and high-risk breaches.

Notification to Affected Individuals

Where there is a high risk to individuals' rights and freedoms, affected individuals shall be informed without undue delay.

The notification should include:

- Nature of the breach
- Likely consequences
- Actions taken by the school
- Advice on protective measures
- Contact details of the DPO

Regulatory Notification

Where required by law, the DPO shall notify the appropriate supervisory authority within 72 hours of becoming aware of the breach.

8. Corrective Actions

Following investigation, corrective actions may include:

- Password resets
- Access permission reviews
- Additional encryption measures
- Recovery of records
- Improved storage arrangements
- Staff retraining
- Revision of procedures
- Technology upgrades

9. Disciplinary Action

Where a breach results from negligence, misconduct or deliberate actions, disciplinary procedures may be initiated in accordance with the Staff Code of Conduct and Disciplinary Policy.

Examples include:

- Unauthorised access of personal data or student grades and/or tempering with these
- Failure to follow reporting procedures
- Deliberate disclosure of confidential information
- Repeated breaches of data protection requirements

10. Record Keeping

The DPO shall maintain a confidential Data Breach Register containing:

- Incident reference number
- Date and time
- Nature of breach
- Individuals affected
- Investigation findings
- Actions taken
- Notification decisions
- Lessons learned

Records shall be retained in accordance with the NIA Data Retention Schedule.

11. Lessons Learned Review

Following closure of every breach investigation:

- A review meeting will be held.
- Root causes will be identified.
- Training needs will be determined.
- Policies and procedures will be updated where necessary.
- Findings will be reported to the Principal and Senior Leadership Team.

12. Annual Review

The DPO will present an annual Data Protection and Data Breach Report to the Principal and Senior Leadership Team, summarizing:

- Number of breaches
- Types of breaches
- Root causes
- Corrective actions taken
- Training completed
- Recommendations for improvement

Approved by: Principal

Responsible Officer: Data Protection Officer

Review Cycle: Annually

Newton Group Values: