NORD ANGLIA EDUCATION

DATA PRIVACY POLICY

This policy covers the collection, use, disclosure, and destruction of Personal Data.

1 September 2023

Version	Issue data
1	7 May 2018
2	September 2023

CONTENTS

1 - INTRODUCTION

This policy applies to the collection, use, disclosure and destruction of Personal Data by the Nord Anglia Education (and all its Schools and corporate entities) and should be adhered to by all Staff. This policy sets the standards of data privacy compliance across NAE, and additional local policies may be required where there is need for additional local requirements.

Any questions or concerns about the operation of this policy should be referred to the Central Compliance Team - Compliance@nordanglia.com.

Data privacy is important to NAE not only because it is a legal requirement but also it is the right thing to do to protect staff, families, students and our stakeholders – please refer to our Code of Conduct and Ethics.

Failure to protect personal data may put these individuals at risk of serious harm, damage our reputation and create a loss of trust. Furthermore, it may lead to civil or criminal penalties to our staff or business and will cause increase in costs to our operations.

2 - SCOPE, AUDIENCE AND DEFINITIONS

This policy and the other policies referred to herein form the overall Data Privacy Policy which supersedes all previous Nord Anglia Education data protection / privacy policies. This policy is for **all staff**.

In this policy, when referring to policy implementation: “must” means required, “should” means strongly recommended and “may” means optional. “Nord Anglia Education”, “NAE”, “we”, “our” and “us” means all schools, offices, business units globally which are under the Nord Anglia Education umbrella.

Definitions of data privacy terminology is set out in Appendix 1.

3 - CORE DATA PRIVACY PRINCIPLES

1. Anyone processing Personal Data must comply with eight principles of compliant processing of Personal Data. These are that Personal Data must be:

    a. processed fairly and lawfully and in a transparent manner (‘lawfulness, fairness & transparency’);
    b. processed for specified, explicit and legitimate purposes (‘purpose limitation’);
    c. adequate, relevant and limited to what is necessary for the purpose (‘data minimisation’);
    d. accurate and where necessary kept up to date (‘accuracy’);
    e. kept in a form which permits identification of the Data Subject for no longer than necessary for the purpose (‘storage minimisation’); and
    f. kept secure using appropriate technical and organisational means (‘security, integrity and confidentiality’);
    g. not transferred to another country without appropriate safeguards (‘transfer limitation’)
    h. allow Data Subjects to exercise certain rights (‘data subject’s rights and requests’)

2. We are responsible for and must be able to demonstrate compliance with the above data privacy principles.

4 - RESPONSIBILITIES & KEY CONTACTS

1. **Everyone** is responsible for upholding this policy and ensuring compliance with this policy.
2. NAE’s Group Data Protection Officer is responsible for keeping this policy up to date, liaising with regulators, and providing assurance to the NAE Board on compliance across the NAE Group.
3. The Central Compliance Team is responsible for day-to-day support and liaise with local Data Protection Officer, where appointed locally.
4. Principals and Heads of Business Units will be accountable for data protection in their School / Business Unit.
5. Local Data Protection Officers are responsible to the Group Data Protection Officer to provide local assurance regarding data privacy compliance.
6. Principals are responsible for appointing a local Data Protection Officer or Data Protection Champion and ensuring that they have sufficient time and resources to perform their tasks. Principals will update the Central Compliance with the relevant appointee’s details.

Contact Central Compliance via email – compliance@nordanglia.com

5 - LAWFULNESS, FAIRNESS & TRANSPARENCY

1. Personal data must be processed lawfully, fairly and in a transparent manner.
2. We must only collect, process and share personal data fairly and lawfully and for a specific purpose. Therefore, you need to ensure we have legal grounds for processing personal data. Please see appendix 2 for further explanation on the various grounds for processing.

3. If you are collecting personal data and are uncertain on what legal grounds is the basis for the processing then please speak to your Data Protection Officer (where relevant), the Central Compliance Team (compliance@nordanglia.com) or your local legal team before proceeding.
4. When processing Special Categories of Personal Data (relating to health, political or religious beliefs, ethnicity, etc.), we should require explicit consent. If you are not relying on explicit consent, then you must consult with your Data Protection Officer (where relevant) or the Central Compliance Team (compliance@nordanglia.com) or your local legal team prior to processing this data.
5. Each School and Business Unit must document the legal ground being relied on for each processing activity including, where legally required, a data processing register must be maintained (e.g. Europe/Thailand/Ecuador, etc.). These must be updated at a minimum annually and shared with the Central Compliance Team.
6. The Central Processing Register will be maintained by the Central Compliance Team and all Central Services staff must notify the Central Compliance Team if there are any updates to existing data processing or new processing activities or data processors.
7. When relying on Consent we must ensure that the Consent Protocol is adhered to as set out in appendix 3.
8. Data Subjects must be provided with a privacy notice / personal information collection statement ("PICS") which must be based on the current Central Compliance Team issued template and meet local data privacy regulations / laws. These should include:
   a. the identity of the Data Controller(s);
   b. purpose for which we are processing their personal data;
   c. source of the data and legal grounds for processing;
   d. categories of recipients of the personal data;
   e. whether their personal data will be transferred internationally and any relevant safeguards;
   f. how long we retain personal data for;
   g. what their rights are.

   Always check the requirements with your Data Protection Officer, where relevant, or local legal advisers. For Schools, you must ensure that the privacy notice accurately reflects that the school is part of the NAE Group and must reflect the roles of Nord Anglia Education Limited and affiliates in any such notice as controllers and processors in addition to the School (e.g. Nord Anglia Education Limited organises Expeditions and therefore will be a controller of participating student data when running such activities).

6 - PURPOSE LIMITATION

1. Privacy notices must be provided to Data Subjects every time we collect personal data from them or when we first communicate with them. Any revisions should be brought to their attention appropriately.
2. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner which is incompatible with those purposes.

7 - DATA MINIMISATION

1. Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
2. You may only collect Personal Data that you require for your job duties and must not process Personal Data for any reason unrelated to your job duties; do not collect excessive data.
3. You must ensure any Personal Data collected is adequate and relevant for the intended purpose.
4. You must ensure that when Personal Data is no longer needed for a specific purpose, it is deleted or anonymised in accordance with the relevant Data Retention Schedule – Please refer to the Data Retention Policy for further information.

8 - ACCURACY

1. Personal Data must be accurate and kept up to date. It must be corrected or deleted without delay when inaccurate.

2. Steps must be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data in respect of any system, register or other process for which processes Personal Data that you are responsible.

9 - STORAGE MINIMISATION

1. Personal Data must not be kept longer than is necessary for the purposes for which that data was collected and is processed.
2. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.
3. Each Central Department provide the Central Compliance Team their data retention requirements and ensure Personal Data is deleted after an appropriate time unless a law requires that data to be kept for a minimum period. They must regularly review their data retention requirements annually.
4. Each School and Business Unit will maintain a local data retention schedule and associated procedures to ensure Personal Data is deleted after an appropriate time unless a law requires that data to be kept for a minimum period. This must be regularly reviewed, and a copy shared with the Central Compliance Team.
5. Each global database / system owner must ensure their database / system can facilitate data retention periods and allow in certain circumstances to hold-off deletion of data.
6. The Central Compliance Team will maintain the Central retention schedule and the Data Retention Policy. Each database owner must conduct regular audits and erasures in line with the relevant data retention schedule and, if relevant, provide adequate training to school database administrators to enable local erasure in line with local data retention schedules.
7. You must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the applicable records retention schedules and policies. This includes requiring third parties to delete the data where applicable. You should obtain certification or formal confirmation of the destruction from any third party.

10 - SECURITY, INTEGRITY & CONFIDENTIALITY

1. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction, or damage.
2. You must adhere to the IT Security Policy. Central IT will ensure that the policy is maintained with appropriate safeguards proportionate to our size, scope and business, the amount of Personal Data that we own or maintain and identified risks (including use of encryption and pseudonymisation, where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.
3. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.
4. You must exercise particular care in protection of Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure. These must have additional protections put in place, such as restricting access to a small group of staff, using specific software to secure the data (e.g. safeguarding data only stored on safeguarding software), encrypting at rest with high level of encryption. Please refer to the IT Security Policy and the Safeguarding Guidance.
5. You must follow all procedures and technologies we put in place to maintain security of all Personal Data from the point of collection to the point of destruction.
6. You may only transfer Personal Data to a third-party service provider who agrees to comply with the required policies and procedures and who have and/or agree to put in place adequate measures, as requested.
7. You must maintain data security by protecting the confidentiality, integrity, and availability of Personal Data, defined as follows:
    a. **Confidentiality:** only people who have a need to know and are authorised to use the Personal Data can access it on a least privilege basis;

b. **Integrity:** Personal Data is accurate and suitable for the purpose for which it is processed; and
c. **Availability:** authorised users can access the Personal Data when they need it for authorised purposes.

8. You must not attempt to circumvent the administrative, physical and technical safeguards implemented by Nord Anglia Education.

11- REPORTING A PERSONAL DATA BREACH

1. Data protection laws may require us to notify any Personal Data Breach to a relevant regulator and in certain instances a Data Subject. It is essential that any suspected or actual breach is reported to the Group and, if relevant, local Data Protection Officer **immediately**.
2. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so. This will only be done with the prior authorisation of the Group Data Protection Officer.
3. Our Personal Data Breach Protocol must be followed in any suspected or actual Personal Data Breach. This may run in parallel to a Security Incident as defined in the IT Security Policy, if relevant. Please note that not all Personal Data Breaches are also Security Incidents and vice versa. Any Security Incident which is suspected to involve Personal Data, must be treated as a Personal Data Breach also.
4. Do not attempt to investigate the matter yourself. You should preserve all evidence relating to any potential Personal Data Breach and must cooperate with the Global and local Data Protection Officers.

12 – TRANSFER LIMITATION

1. A transfer of Personal Data occurs when that data is transmitted, sent, viewed, or accessed in or to a different country to where it originated.
2. You must adhere to the international data transfer restrictions and compliance requirements for your country. If you are unsure of the rules, then you should consult with the local Data Protection Officer, if applicable, local legal team or the Central Legal and Compliance Teams to assess the requirements and advise you.
3. You must comply with any cross-border / international data transfer procedures issued by NAE.
4. **EU Schools**
   a. You have restrictions to transfer Personal Data outside of the EEA, except to countries which have been deemed adequate by the European Commission – a list can be found on their website.
   b. You must also ensure that the transfer is necessary, and you have assessed the adequacy of the protections to where you are transferring the data and ensure that there are the appropriate contractual protections in place (using the Standard Contractual Clauses ("**SCC**") in your data processing / supplier contract/agreement). If you need support in these please reach out to your Data Protection Officer. Note all EU schools have a Data Protection Officer appointed.
   c. ***Non-EU School's use of SCC***: Certain countries allow reliance on the SCC to effect transfers. Please speak with your local Data Protection Officer or local legal team to ensure that there are adequate clauses to incorporate the SCC to the local context.
5. **UK Schools**
   a. You have restrictions to transfer Personal Data outside of the UK and EEA, except to countries which have been deemed adequate by the UK's Information Commissioner's Office – a list can be found on their website.
   b. You must also ensure that the transfer is necessary, and you have assessed the adequacy of the protections to where you are transferring the data and ensure that there are the appropriate contractual protections in place (using the International Data Transfer Agreement ("**IDTA**") in your data processing / supplier contract/agreement). If you need support in these please reach out to your Data Protection Officer.
6. **Central Services**
   a. You must ensure that at a minimum both EU & UK international data transfer terms (e.g. SCC & IDTA) are in place for an international data transfer and with due consideration for all other jurisdictions in which NAE operates. Seek support from the Central Legal and Compliance Teams.

13 – DATA SUBJECT'S RIGHTS & REQUESTS

1. A Data Subject has rights when it comes to how we handle their Personal Data. These may include rights to:
   a. withdraw consent to processing at any time;
   b. receive certain information about our processing activities;
   c. request access to their Personal Data that we hold;
   d. prevent our use of their Personal Data for direct marketing purposes;
   e. ask to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or rectify inaccurate data or to complete incomplete data;
   f. restrict processing in specific circumstances;
   g. challenge processing which has been justified on the basis of legitimate interest or in the public interest;
   h. request a copy of an agreement which covers the international transfer of Personal Data;
   i. object to any automated decision making;
   j. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
   k. make a complaint to the supervisory authority; and
   l. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structure, commonly used and machine-readable format.

   These rights will vary from country to country and NAE will adhere to the rights of Data Subjects relevant to the country they are in.
2. You must verify the identity of the individual requesting data under any of the rights above. Do not allow third parties to persuade you to disclose Personal Data without proper authorisation.
3. You must immediately forward any Data Subject request you receive to your local Data Protection Officer, if applicable, or the Global Data Protection Officer. Please refer to the Subject Rights Request Guidelines Overview for further information and guidance.

14 – ACCOUNTABILITY

1. We must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. Each School and Business Unit is responsible for and must be able to demonstrate compliance with this Data Privacy Policy and the principles contained herein.
2. We must have adequate resources and controls in place to ensure and to document data privacy compliance, including:
   a. appointing a suitable (and qualified) Data Protection Officer, where legally required and necessary, or at a minimum a Data Protection Champion;
   b. implementing Privacy by Design and completing Data Protection Impact Assessment ("**DPIA**") where processing presents a high risk to the rights and freedoms of Data Subjects;
   c. integrating data privacy into other internal documents/policies and procedures;
   d. regularly training and improving awareness of data privacy – using NAE training resources and completing any and all mandatory training.
   e. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

15 – RECORD KEEPING

1. We must keep an accurate record of all our data processing activities. You may use the data processing register to record this.
2. You must keep and maintain accurate records reflecting our processing including records of Data Subject consents and the procedures for obtaining consents.
3. Any processing registers should include, at a minimum, clear description of:
   a. the Personal Data types;
   b. the Data Subject types;
   c. the processing activities;
   d. the processing purposes;

e. third-party recipients of the Personal Data;
f. Personal Data storage locations;
g. Personal Data transfers;
h. Personal Data retention periods; and
i. security measures in place.

4. You should create data maps which should include the above detail with appropriate data flows.

16 – TRAINING AND AUDIT

1. We are required to ensure all NAE staff have undergone adequate training to enable them to comply with data privacy laws.
2. We must regularly test our systems and processes to assess compliance.
3. You must undertake all mandatory data privacy and cyber security training and ensure your team maintains good awareness of data privacy and cyber security.
4. You must regularly review all systems and processes under your control to ensure they comply with this Data Privacy Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

17 – PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT

1. We are required to implement Privacy by Design as a default when processing Personal Data by implementing appropriate technical and organisational measure (e.g. pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
2. You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process Personal Data by taking into account the following:
   - The state of the art.
   - The cost of implementation
   - The nature, scope, context and purposes of processing.
   - The risks on the rights and freedoms of Data Subject posed by the processing (with due regard for the impact and likelihood of the risk).
3. We must conduct a Data Protection Impact Assessment ("DPIA") when implementing a major system or business change programme involving the processing of Personal Data including:
   a. Use of new technology or changing technologies.
   b. Automated processing including profiling or automated decision making.
   c. Large-scale processing of Special Categories or Personal Data or Criminal Convictions Data.
   d. Large-scale, systematic monitoring of a publicly accessible area.
4. You should use the NAE DPIA template to complete your assessment and it must be carried out prior to the implementation of the new system and/or change. All Central DPIA's will require review by the Central Compliance Team and Cyber Security Team, prior to completion of the DPIA.

18 – AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

1. Generally, this activity is prohibited when a decision based on the automated process has a legal or similar significant effect on an individual unless the Data Subject has consented, the processing is authorised by law or is necessary for the performance of or entering into a contract.
2. This type of processing includes the use of AI (artificial intelligence) and is automatically considered a high risk form of processing. This means that you must ensure that a Data Privacy Impact Assessment is carried out prior to this processing taking place.
3. Special Categories of Personal Data or Criminal Convictions Data may only be processed in this way with explicit consent, and only where there is a substantial public interest (e.g. fraud prevention).
4. If you are planning on incorporating any automated processing or automated decision-making, you must contact the Central Compliance Team for advice.

19 – DIRECT MARKETING

1. We are subject to certain rules and regulations when marketing to current and prospective families.

2. Consent is required for electronic direct marketing (e.g., by email, text or automated call).
3. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from the other information. You should keep any electronic 'opt-out' mechanism simple.
4. We must honour objections to direct marketing promptly and ensure the Data Subject is placed on our suppression list to ensure we respect their marketing preferences in the future.
5. Marketing and Admissions teams are responsible to ensure their procedures adhere to these rules.

20 – SHARING PERSONAL DATA

1. We are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
2. You may only share Personal Data with another employee, agent, or representative of NAE if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restriction.
3. You may only share Persona Data we hold with a third party, such as our service provider, if:
   a. they need to know the information for the purposes of providing the contracted services;
   b. sharing the Personal Data complies with our privacy notices provided to the Data Subject and, if relevant, the Data Subject's consent has been obtained;
   c. the third-party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
   d. the transfer complies with any applicable cross-border transfer restrictions; and
   e. a fully executed contract containing the necessary data privacy clauses (as contained in NAE's data processing templates) has been obtained.
4. We may receive requests for Personal Data from law enforcement agencies, regulators, local authorities or other public bodies, and we may receive requests as part of civil litigation (e.g. family disputes). Ln each local country there must be a process in place to verify that the sharing is lawful and ensure that we comply with local legal requirements in sharing that data – please speak to your local Data Protection Officer or local legal team. In these circumstances, we are unlikely to be able to give notice to individuals of the data sharing and may be barred from doing so. Where possible, notice of these requests must be provided to the Central Compliance Team.
5. NAE may be requested to provide data based on a public interest, in which case, NAE must assess whether there is a genuine public interest balancing with individual rights. These decisions must be recorded in writing and prior notification must be provided to the Central Compliance Team.

21 – CHANGES TO THIS DATA PRIVACY POLICY

1. We keep this Data Privacy Policy under regular review. Historic versions are available from the Central Compliance Team.
2. This Data Privacy Policy does not override any applicable national data privacy laws and regulations in countries where NAE operates. Certain countries may require a localised variance to this Data Privacy Policy, which are available from the local Data Protection Officer.

APPENDIX 1

DEFINITIONS

Automated Decision-Making: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Process: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be unambiguous indication of the Data Subject's wishes by which they, by a statement or a clear positive action, signify agreement to the processing of Personal Data relating to them.

Controllers: the person or organisation that determines when, why and how to process Personal Data It is responsible for establishing practices and policies in line with relevant legislation. We are the Controller of all Personal Data relating to our staff, and Personal Data used in our business for our won commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Privacy Champion: a person designated to champion data privacy in a Business Unit / School fulfilling a similar role to a Data Protection Officer while not appointed under a specific data privacy law with the same restrictions.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activities. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of Personal Data.

Data Protection Officer: either of the following:

- The person appointed in specific circumstances under data privacy law (e.g., GDPR); or
- Where a mandatory Data Protection Officer has not been appointed, a data privacy manager or other voluntary appointment of a Data Protection Officer or Data Privacy Champion.

Data Subject: a living, identified, or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: European Economic Area which includes all EU countries and also Iceland, Liechtenstein and Norway

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data along or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and pseudonymised Personal Data but excludes anonymous data that has had the identity of an individual permanently removed. Personal data can be factual or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the relevant data privacy laws (e.g. GDPR, PDPA, PIPL, etc) to any new system / data processing / database prior to implementation.

Privacy notice: separate notices setting out information that may be provided to Data Subjects when NAE collects information about them. These notices may take the form of:

- general privacy statement applicable to a specific group of individuals (e.g. employee privacy notice or website privacy notice); or
- standalone, onetime privacy statement covering processing related to a specific purpose.

Processing or process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties or within NAE.

Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data / Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

APPENDIX 2

GROUNDS FOR PROCESSING

Use of Personal Data must be justified under one legal basis and we are required to set out the legal basis in our privacy notices. Please note there are different grounds for general Personal Data, Special Categories of Personal Data and Criminal Convictions Data.

Please note that these are general Grounds for processing and can differ between jurisdictions – therefore speak to your local Data Protection Officer or get in touch with the Central Compliance Team.

General

Contract performance: where the Personal Data is necessary to enter into or perform our contract with the Data Subject.

Legal obligation: where we need to use Personal Data to comply with our legal obligations.

Legitimate interests: where we use Person Data to achieve a legitimate interest and our reasons for using it outweigh any prejudice to the Data Subject data privacy rights. Note that to rely on this we will need to document our assessment. Reach out the Central Compliance Team or your local Data Protection Officer, if you need assistance.

Legal claims: where Personal Data is necessary for us to defend, prosecute or make a claim against Data Subjects, us or a third party.

Public Interest/Task: process Personal Data in the exercise of official authority or to perform a specific task in the public interest that is set out in law. For example, at a NAE school this could be tasks that a public school authority would undertake which the school is obliged to also perform.

Consent: where a Data Subject has consented to the processing of their Personal Data for one or more specified purposes.

Vital interest: where we need to process Personal Data in an emergency to protect someone's life and they are incapable of consenting.

Special Categories of Personal Data

Employment, social security and social protection: where processing is necessary for the obligations in employment, social security and social protection law.

Vital Interest: Processing is necessary to protect the vital interests of the Data Subject or of another, where the Data Subject is physically or legally incapable of consenting.

Legal claims: Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.

Substantial public interest: Processing is necessary for reasons of substantial public interest, on the basis of a local law.

Health or Social care: to assess Data Subjects working capacity, assist in making medical diagnoses, or provision of health/social care and treatment. Social care includes social work, personal care and social support services. Includes school nurses, speech language therapists, child psychologist, etc.

Made public by the Data Subject: where the Data Subject has manifestly made public the Personal Data. E.g. a Parent is a member of a national Parliament for a specific political party ('political beliefs').

Public Health: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

Explicit consent: Data Subject has given explicit consent to the processing of their Personal Data for one or more specified purposes.

Criminal Convictions Data

Processing is only allowed under the control of official authority or when the processing is authorised by local laws. Please speak to your local DPO to understand when we can process Criminal Convictions Data or reach out to the Central Compliance Team.

APPENDIX 3

CONSENT PROTOCOL

- A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly by a statement or positive action to the Processing.
- Consent requires affirmative action, so silence, pre-ticked boxes or activity are unlikely to be sufficient.
- If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
- A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.
- Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which as not disclosed when the Data Subject first consented.
- You must evidence Consent captured and keep records of all Consents – you need to design your processes to enable us to capture and use evidence of Consent as and when necessary.