Logo, company name

Description automatically generated

**CONFIDENTIALITY AND DATA PROTECTION POLICY**

A guide for all staff, trustees, and volunteers

This policy will be reviewed on an ongoing basis, at least once a year. NAPA will amend this policy, following consultation, where appropriate.

Date of last review: 02/06/2021

Contents  
[General Principles](#generalprinciples)  
[SAAS Coordinate and NAPA Account Holders Privacy Agreement](#privacynotice)  
[Why information is held](#whyinformationisheld)  
[The Data Protection Act](#dataprotectionact)  
[What is data protection?](#whatisdataprotection)  
[The law](#thelaw)  
[Consequences of breaching the data protection act](#consequences)  
[The eight data protection principles](#theeight)  
[Access to information](#accesstoinformation)  
[Parents’ access to files](#parentsaccesstofiles)  
[Employee access to records](#employeeaccesstorecords)  
[Storing information](#storinginformation)  
[Duty to disclose information](#dutytodisclose)  
[Disclosures](#disclosures)  
[Breach of confidentially](#breach)  
[Further information](#furtherinformation)

Confidentiality and Data Protection Policy

**General principles**

NAPA recognises that employees, volunteers, trustees & others who work within our organisation gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential, and we may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

NAPA is committed to ensuring that any personal information which is provided to us in the course of our work will be processed and stored in accordance with the Data Protection Act.

Confidentiality is a broader concept than data protection but there is overlap between the two areas.

**Confidentiality** refers to all forms of information including personal information about people using services or employees or volunteers, information about the organisation, for example, its plans or finances and information about other organisations, whether the information is recorded or not.

**Data protection** concerns only personal information, which is recorded, whether this be in electronic or manual format.

Information received by NAPA as part of the services it provides will be considered to be information for NAPA to share with colleagues and use to deliver its aims and objectives. Personal information on account holders (parents) and participants (children) will be held within our secure Coordinate database and payment system. This database is held with SAAS Coordinate Ltd.

When registering with NAPA, all parents are required to tick a box to say that they have read, and agree to, the following terms and Privacy Policy:

PRIVACY NOTICE  
REGARDING DATA HELD BY NORTHERN ACADEMY OF PERFORMING ARTS

1 - This notice is intended to inform you about the information that we hold in relation to you, why we hold it, for how long and your rights in respect of the right in certain circumstances to ask us to delete information or to anonymise any papers that we hold on your files. The law regarding this is contained in Regulation (EU) 2016/679 of The European Parliament and of The Council. The regulations are known as the EU General Data Protection Regulation (GDPR).

2 - The responsible entity: Coordinate SaaS Limited and its officers are responsible to you for the privacy of your data and the safe and proper handling of it.

3 - Compliance: Any clients, customers or suppliers are Data Controllers under GDPR and Coordinate Saas Limited is the Data Processor. Both Data Controllers and Data Processors are obliged to comply with the GDPR, and we rely on your attention and observance where required.

4 - Employees: Coordinate SaaS Limited ensures that all of its employees are aware of the confidential nature of Personal Data, have adequate training in relation to the data protection legislation and that they are bound by relevant obligations and restrictions when processing Personal Data.

5 - Any use that we make of your data must be fair and lawful. We will hold all confidential and personally identifiable information and data concerning our clients, customers, suppliers, and partners securely and in confidence using appropriate technical and organisational measures.

6 - We will only use your data for the purposes for which it was provided under the applicable terms of business and to comply with any statutory requirements upon us.

7 - Except as set out in paragraph 8 and 14 below, your information and data will NEVER be passed on to another organisation under any circumstances.

8 - When required we may provide relevant data to other parties such as to our accountants for the purposes of providing our accounting services to us and to enable us to comply with any audit requirements generally. All such parties have stringent data processing obligations, and they are not authorised to use your data other than for the purposes of the reference/accounts/audit as above mentioned.

9 - On occasion, we may use your data to contact you to find out if you have been satisfied with the work carried out on your behalf or to let you know of any events or offers that we may wish you to be aware of. Please notify us if you do not wish to be contacted in this way.

10 - We may on occasion place marketing materials on to our website or Social Media sites. If you do not wish us to place anything incorporating your photograph (e.g. as part of a group photo at an event) please let us know. We will always respect your wishes.

11 - SAR Requests: We will handle subject access requests (SAR) promptly, however when we consider SAR’s to be manifestly unfounded, excessive or to adversely affect the rights and freedoms of others, we will refuse the request.

12 - Article 28: If an audit or inspection is required to evidence that Coordinate Saas Limited is meeting its obligations under Article 28, Coordinate Saas Limited will assist appropriately but will inform the Client if it is asked to do something infringing the GDPR or the other UK, EU or member state data protection law.

13 - ICO: Coordinate Saas Limited proposes to co-operate with supervisory authorities (such as the ICO) in accordance with Article 31.

14 - Sub-contractors: The Client has been informed that Coordinate Saas Limited may transfer data to a sub-processor or data controller to fulfil some, or all, of the contract. In these cases, Coordinate Saas Limited will put in place a contract with the processor to adequately protect personal data. The Client consents to this processing.

15 - Data breach: In the event of any personal data breach we will notify our Clients in accordance with Article 33.

16 - Client Instructions: The Client acknowledges that Coordinate SaaS Limited is reliant on the Client for direction as to the extent to which it is entitled to use and process Personal Data. No liability is accepted by Coordinate SaaS Limited for any claim arising from any act or omission by it, to the extent that such act or omission resulted directly from client’s instructions.

17 - Consent and revocation: After reading this notice you are asked to indicate your consent to us continuing to hold your data in the manner and for the purposes above mentioned. Subject as set out below, you are entitled to revoke your consent at any time and if so, we will keep a record of when you asked us to cease processing your data and we will advise you of what continues to be held by us and when we are legally able to delete it.

18 - If you revoke your consent, it may affect the relationship between us and we will not be liable for any consequential issues arising. In certain circumstances, we may be obliged to cease to supply goods or services.

19 - We are legally obliged to hold your information and our files in relation to work carried out for you for up to [6 years] in most cases. You cannot ask us to erase this information.

20 - Contact Us: If you wish to contact us about the use being made of your data, you should send any communication to: napa@northernacademy.org.uk

Staff and volunteers are able to share information with their Head of Department and the Chief Executive in order to discuss issues and seek advice but should not disclose to anyone, other than their manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or the Chief Executive, in the case of an organisation.

Staff, trustees, and volunteers should avoid exchanging personal information or comments (gossip) about individuals with whom they have a professional relationship.

Staff, trustees, and volunteers should avoid talking about organisations or individuals in social settings.

There may be circumstances where it would be appropriate for colleagues to discuss difficult situations with each other to gain a wider perspective on how to approach a problem.

If staff and volunteers receive information from individuals outside NAPA regarding the conduct of a colleague, then this should be dealt with sensitively. The appropriate colleague should tell the individual about the Complaints Procedure and advise them accordingly.

If employees are dissatisfied with the conduct of a colleague, and have sensitive information that could be evidenced through investigation, they should discuss it with

The Chief Executive. Any allegation, which is found to be malicious, or ill-founded, will be dealt with by the Chief Executive action under the Disciplinary Procedure.

Where there is a legal duty on NAPA to disclose information, the person that is affected will be informed that disclosure has or will be made.

**Why information is held**

Most information held by NAPA relates to individuals or students, members, employees, trustees, and volunteers.

Information is kept to enable NAPA’s staff to deliver classes, take payments for classes and contact parents/emergency contacts in an emergency.

Information about participants may be kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

**Data Protection Act**

The 1998 Data Protection Act came into force on 1 March 2000. The purpose of the Act is to protect the rights of individuals about whom data (information) is obtained, stored, processed, and disclosed.

**What is data protection?**

Data protection is essentially that area of the law that governs what may, and what may not, be done with personal information. Such personal information may be in electronic (e.g., stored on computer hard drive) or manual form (in a manual filing system).

**The law**

The Data Protection Act is mandatory, and NAPA is required under law to comply with the Act. This means that we must:

- Notify and register with the Information Commissioner’s (IC) Offices

- Adhere to the eight data protection principles below

- Educate and train staff in the correct use of data

**Consequences of breaching the Data Protection Act**

Staff can be criminally liable if they knowingly or recklessly disclose personal data in breach of the Act.

A serious breach of data protection is also a disciplinary offence and will be dealt with under the NAPA’s disciplinary procedures. If a member of staff accesses another employee’s personnel records without authority this constitutes a gross misconduct offence and could lead to summary dismissal.

**Notification**

The Information Commissioner maintains a public register of data controllers who process data (information) and who are required to notify their details to the Commissioner.

**The Eight Data Protection principles**

There are eight principles of data (information) processing with which the data controller must ensure compliance. In this instance NAPA is the ‘data controller’.

Personal data shall be:

**Principle 1:** processed fairly and lawfully

**Principle 2:** obtained only for the purpose stated

**Principle 3:** adequate, relevant and not excessive

**Principle 4:** accurate and, where necessary, kept up to date

**Principle 5:** not be kept for longer than is necessary for that purpose

**Principle 6:** processed in accordance with the rights of data subjects under the Act

**Principle 7:** appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data

**Principle 8:** not transferred to countries without adequate protection

**Access to information**

Information is confidential to NAPA as an organisation and may be passed to colleagues, line managers or trustees to ensure the best service for parents and participants.

Sensitive information involving disputes or legal issues will be confidential to the employee dealing with the case and the Chief Executive.

Employees and volunteers will not withhold information from their line manager unless it is purely personal to them and not business related.

**Parent access to files**

Parents may see NAPA records which relate to them, but only the information about themselves. The letter must be signed by the individual.

The records must be provided ‘promptly’ and in any event within 40 days.

**Employee access to records**

Employees may see all of their personnel records by giving 14 days’ notice in writing to the Chief Executive. The letter must be signed by the individual.

**Storing information**

The majority of personal information stored on parents and participants will be kept on NAPA’s secure database, Coordinate.

Additional confidential information will be kept in locked cabinets and in the case of electronic records, password protected.

NAPA will ensure that only authorised people have access to confidential records.

**Duty to disclose information**

NAPA has a legal duty to disclose some information including:

Child abuse, drug trafficking, money laundering, acts of terrorism or treason and other criminal activities where others may be at risk.  
  
**Disclosures**   
NAPA will request Enhanced Disclosure and Barring Service (DBS) checks for all new employees and volunteers and will comply fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

**Breach of confidentiality**

Staff and volunteers who are dissatisfied with the conduct or actions of other colleagues or NAPA should raise this with the Chief Executive as a grievance if necessary, and not discuss their dissatisfaction outside of NAPA.

Employees accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

**Further Information**

The Information Commissioner’s Office has a guide to Data Protection. See www.ico.org.uk/for\_organisations/data\_protection/the\_guide