Data Protection Policy

1.0 Aims

The NFA Group aims to ensure that all personal data held about children, young persons, foster carers, employees and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill 2017.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2.0 Legislation and guidance

This policy aims to meet the requirements of the GDPR and the expected provisions of the DPA 2018 and is based on guidance published by the Information Commissioner's Office (ICO) and the Article 29 Working Party.

3.0 Key terms

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's:- • Name (including initials) • Identification number • Location data • Online identifier, such as a username
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's:- • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	An incident, breach or 'near miss' leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 The role of the Data Controller

The NFA Group and its companies (including fostering agencies, schools and residential homes) process personal data relating to children, young persons, foster carers, employees and other individuals, and therefore is a data controller.

Each individual company, fostering agency and school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.0 Roles and responsibilities

This policy applies to all employees of the NFA Group, and to external organisations or individuals working on our behalf (such as contractors, panel members, independent reviewers etc.). Where this policy refers to 'employees', this term is used to be inclusive of employees and those who work on our behalf. It does not confer employment rights on these individuals. Those who do not comply with this policy may face disciplinary action.

5.1 NFA Group Board and Executive Team

The Board and Executive Team have overall responsibility for ensuring that the NFA Group complies with all relevant data protection obligations. Both groups will in receipt of regular updates.

5.2 Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on data protection issues within the NFA Group.

The DPO is also the first point of contact for individuals whose data the NFA Group processes, and for the ICO.

Our DPO is Paul Walker and is contactable via DPO@nfa.co.uk.

5.3 Information Management Strategy Group and Data Protection & Information Security Operational Group

Both the Strategy Group and the Operational Group support the NFA Group's commitment to the development, management and accountability of the group's approach to Information Management, Data Protection and Information Security.

5.4 All employees and those working on our behalf

Are responsible for:-

- Collecting, storing and processing any personal data in accordance with this policy
- Informing HR of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:-
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity or process that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6.0 Data protection principles

The GDPR is based on data protection principles that the NFA Group must comply with.

The principles say that personal data must be:-

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the NFA Group aims to comply with these principles.

7.0 Collecting personal data

We will only process personal data where we have a legal basis to do so under data protection law:-

- The data needs to be processed so that the NFA Group can fulfil a contract with the individual, or the individual has asked the NFA Group to take specific steps before entering into a contract
- The data needs to be processed so that the NFA Group can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed for the legitimate interests of the NFA Group or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate) has freely given clear explicit consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and the expected provisions of the Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will only collect personal data for specified, explicit and legitimate reasons. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Employees must only process personal data where it is necessary in order to do their jobs.

8.0 Sharing personal data

We will not normally share personal data with anyone else, but if we do, any sharing we do will be in accordance with the law. Examples of this are (please note that this list is not exhaustive):-

- There is an issue with a child/young person or parent/foster carer that puts the safety of the people we work with at risk
- We need to liaise with other agencies in terms of a placement
- To highlight safeguard concerns and make appropriate referrals

Our suppliers or contractors may need data to enable us to provide services to our placements, pupils and employees – for example, IT companies, confidential waste disposal, employee benefits etc. When doing this, we will:-

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreements (or similar) with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:-

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children, young persons, residents, foster carers or employees.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9.0 Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a qualified right to make a 'subject access request to gain access to personal information that the NFA Group holds about them (subject to exemptions). This includes:-

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing. They should include:-

- Name of individual
- Proof of identity
- Correspondence address
- Contact number and email address
- Details of the information requested

If an employee receives a subject access request they must notify the DPO and seek advice on how to progress.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not automatically that of the child's parents or carers.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children or young persons may be granted without the express permission of the child or young person.

Children and young persons aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children or young persons may not be granted without the express permission of the child or young person.

These are not rules and ultimately a child or young person's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:-

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

There will often be reasons why we cannot disclose information, these will be communicated to the requestor.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7.0), individuals also have the right to:-

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. However, if employees receive such a request, they must consult with the DPO to identify a way forward.

10.0 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:-

- The appointment of a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Protection Impact Assessments (DPIA) where the NFA Group's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly train those employed/engaged by the NFA Group on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:-
    - For the benefit of data subjects, making available the name and contact details of the NFA Group and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

11.0 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:-

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access NFA Group computers, laptops and other electronic devices. System users are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

12.0 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the NFA Group's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

13.0 Personal data breaches

The NFA Group will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach or near miss, we will follow the procedure set out in Appendix A.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:-

- access by an unauthorised third party (i.e. our systems exposed as a result of a cyber attack)
- deliberate or accidental action (or inaction) by a controller or processor (i.e. an employee using their personal email account to conduct work business)
- sending personal data to an incorrect recipient (i.e. an email sent to another person by mistake)

- computing devices containing personal data being lost or stolen (i.e. your laptop or phone being lost or stolen)
- alteration of personal data without permission (i.e. you notice that records have been amended without appropriate reason or authorisation)
- significant loss of availability of personal

If you are unsure whether to report, it is advised that you report anyway to be advised accordingly.

14.0 Training

All those employed by the NFA Group are provided with data protection training and completion of this is mandatory.

15.0 Acceptable use of IT equipment

All NFA Group employees should be aware of the provisions of the following policies:-

- Email and Internet Policy
- IT Security Policy
- IT Equipment and Systems Usage Policy

Failure to comply with these policies will result in disciplinary action. For copies of these policies, please contact IT, the DPO or check your intranet pages.

16.0 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed every 12 months.

Please ensure you are referring to the latest version of this policy.

Author	Data Protection Officer
Document Title	Data Protection Policy
Review Date	May 2019

Appendix A: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the employee or data processor must immediately notify the DPO. The DPO can be contacted on 01204 556344. If there is no answer call the IT Service Desk on 01204 556331. To report breaches out of hours (24/7), please call 07815 577011.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:-

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people
- Made inaccessible

The DPO will alert the relevant Senior Manager (i.e. Head of Service, Headteacher, responsible Director etc.).

The DPO will offer containment advice to minimise the impact of the breach. Containment action will be completed by the service area in which the breach occurred.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will decide if the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:-

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision whether to report to the ICO (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of the group becoming aware of the incident. As required, the DPO will set out:-

- A description of the nature of the personal data breach including, where possible:-
    - The categories and approximate number of individuals concerned

    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO (in collaboration with senior management from the effected service area) will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:-

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO or the employee in the service area in which the breach occurred will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:-

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

The DPO and relevant stakeholders will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.