**Neil Fuller & Associates**

**Data Protection Policy**

**1 Introduction**

The purpose of this policy document is to communicate the approach and policies that NFA adopts while processing data to ensure it complies with the requirements of the Data Protection Act 1998 (DPA) to users of NFA systems and our customers; The DPA is law, and not an optional set of guidelines – we are all responsible in our actions for ensuring that NFA remains within the boundaries of the DPA.

It is important to consider and fully understand the 8 principles (detailed within section 2 of this document) whenever we process data, as well as any additional specific client requested controls that may have been agreed within contractual terms.

Everyone should be cognisant of the data they handle and process, from the point of consideration and awareness of the following:

 where does the data come from

 why do we need it

 how do we process it

 how do we store it

 how do we secure it

 who has access to it

 how long do we retain it

 how do we dispose of it

This policy document applies to all users, which include employees of NFA, associates, apprentices, temporary staff, volunteers and employees of any partner organisations that are undertaking tasks on NFA’s behalf.

Please refer to section 4 of this document for definitions of the terms used within this policy.

**2 Data Protection Principles & Policy**

The DPA principles are defined by the Information Commissioner’s Office (ICO) and form the fundamental principles of NFA’s policy which must be considered when handling all elements of data.

It is vital that all users understand the importance of protecting personal data and they are familiar with this policy, and that they put its security procedures into practice.

All users must ensure they are aware of the following:

 NFA’s duties under the DPA and restrictions on the use of personal data, detailed within this document;

 the responsibilities of all users for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;

 the dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making “phishing” attacks) or by persuading you to alter information when you should not do so;

 any restrictions NFA places on the personal use of its computers and IT systems by staff (to avoid, for example, virus infection or spam).

**2.1 Processing data fairly and lawfully**

The first DPA principle states that “Personal data shall be processed fairly and lawfully”

In practice, it means that you must:

 have legitimate grounds for collecting and using the personal data;

 not use the data in ways that have unjustified adverse effects on the individuals concerned;

 be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

 handle people’s personal data only in ways they would reasonably expect; and

 make sure you do not do anything unlawful with the data.

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Transparency is always important, but especially so in many marketing situations where individuals have a choice about whether they wish to enter into a relationship with you.

If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship or perhaps to try to renegotiate the terms of that relationship.

Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

**2.2 Obtaining data**

The second DPA principle states that “Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”.

This requirement aims to ensure that NFA is open about their reasons for obtaining personal data, and that what NFA do with the information is in line with the reasonable expectations of the individuals concerned.

In practice, the second data protection principle means that you must:

 be clear from the outset about why NFA are collecting personal data and what we intend to do with it;

 comply with the Act’s fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;

 comply with what the Act says about notifying the Information Commissioner; and

 ensure that if NFA wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

**2.3 Appropriate and relevant data**

The third DPA principle states that “Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.

In practice, it means you should ensure that:

 NFA only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and

 NFA does not hold more information than it needs for that purpose.

So you should identify the minimum amount of personal data NFA need to properly fulfill the purpose. NFA should hold that much information, but no more. This is part of the practice known as data minimisation.

**2.4 Maintaining data**

The fourth DPA principle states that “Personal data shall be accurate and, where necessary, kept up to date”.

Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data NFA receive. So the DPA makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

 take reasonable steps to ensure the accuracy of any personal data you obtain;

 ensure that the source of any personal data is clear;

 carefully consider any challenges to the accuracy of information; and

 consider whether it is necessary to update the information.

**2.5 Retention of data**

The fifth DPA principle states that “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

DPA does not set out any specific minimum or maximum periods for retaining personal data.

In practice, it means that NFA need to:

 review the length of time NFA keep personal data;

 consider the purpose or purposes NFA hold the information for in deciding whether (and for how long) to retain it;

 securely delete information that is no longer needed for this purpose or these purposes; and

 update, archive or securely delete information if it goes out of date.

**2.6 Individual’s rights**

The sixth DPA principle states that “Personal data shall be processed in accordance with the rights of data subjects under this Act”.

In practice this means that individual’s rights are primarily comprised of:

 a right of access to a copy of the information comprised in their personal data (SAR)

 a right to object to processing that is likely to cause or is causing damage or distress;

 a right to prevent processing for direct marketing;

 a right to object to decisions being taken by automated means;

 a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and

 a right to claim compensation for damages caused by a breach of the Act.

**2.7 Securing data**

The seventh DPA principle states that “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”.

In practice, it means NFA must have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. In particular, NFA needs to:

 design and organise our security to fit the nature of the personal data NFA hold and the harm that may result from a security breach;

 be clear about who within NFA is responsible for ensuring information security;

 make sure NFA have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff;

 be ready to respond to any breach of security swiftly and effectively.

There is no “one size fits all” solution to information security. The security measures that are appropriate for an organisation will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security NFA need to implement.

It is important to understand that the requirements of the DPA go beyond the way information is stored or transmitted. The seventh data protection principle relates to the security of every aspect of NFA’s processing of personal data.

Every security measure put in place must ensure that:

 only authorised people can access, alter, disclose or destroy personal data;

 those people only act within the scope of their authority;

 if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

 it is appropriate to the nature of the information in question;

 it is commensurate to the harm that might result from its improper use, or from its accidental loss or destruction.

Physical and technological security is likely to be essential, but is unlikely to be sufficient in itself. Management and organisational security measures are likely to be equally important in protecting personal data.

**2.8 Transfer of data to another country**

The eighth DPA principle states that “Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.

A transfer could be when you email someone information, in the body of the email or as an attachment. This would also apply to the posting or courier of a DVD (or other media such as a USB memory key) containing personal information to a destination outside of the EEA.

This is the eighth data protection principle, but other principles of the DPA are also relevant to sending personal data overseas. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using subcontractors abroad.

Before making a data transfer outside of the EEA, you should consider whether you can achieve your aims without actually processing personal data. For example, if data is made anonymous so that it is not possible to identify individuals from it, now or at any point in the future, then the data protection principles will not apply and you are free to transfer the information outside the EEA.

The DPA does not prohibit transfers of data outside of the EEA. If NFA need to transfer data to companies where the data physically resides in a non-EEA country, then we must ensure that the appropriate controls are in place to provide the same level of data protection that would exist within NFA’s own systems.

**3 Policy Breach**

Should a breach of security occur despite the measures NFA have taken to secure data, it is important that NFA deal with the security breach quickly and effectively.

A data security breach can happen for a number of reasons:

 Loss or theft of data or equipment on which data is stored

 Inappropriate access controls allowing unauthorised use

 Equipment failure

 Human error

 Unforeseen circumstances such as a fire or flood

 Hacking attack

 Blagging’ offences where information is obtained by deceiving the organisation who holds it

NFA undertake the following four elements when managing a reported breach:

**3.1 Containment and recovery**

The first step following a reported breach is to confirm the event and understand the set of circumstances that allowed the breach to happen. The root cause may be a process that requires revision or a technical element that requires modification.

Where the incident cannot be fully resolved immediately, the means by which the breach occurred will be isolated – thus if technical, the failing element should be disabled so that no further breaches can occur, and if a caused by a process, that process must be immediately ceased.

Once the breach is contained, the element leading to the breach will be analysed and enhanced to prevent future breaches.

**3.2 Assessment of on-going risk**

Once the incident is contained, we must assess the risk and consequence of the breach.

The breach will be analysed so that NFA understand the type of data involved and the points below assessed:

 What type of data is involved?

 How sensitive is the data (may be financial, personal or general)?

 If data has been lost or stolen, are there any protections in place such as encryption?

 What has happened to the data?

Regardless of what happened to the data, it is important that the contents are understood so that overall risk is quantified. For example, sensitive data could mean very little to an opportunistic laptop thief whereas the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

The scope of the breach is also quantified so that NFA understand the extent of the risk – for example, is the data limited to one person or a number of people?

The assessment also considers the possible harm that could come to those individuals. This is especially important if the breach puts at risk physical safety or reputation, or financial loss or a combination of these or other aspects of their life.

**3.3 Notification of breach**

When considering notification of the breach to the affected users, NFA will consider the following:

 Are there any legal or contractual requirements?

 Can notification help the individual, such as requesting the user makes password changes?

 If a large number of people are affected, or there are very serious consequences, we should inform the ICO.

 Consider how notification can be appropriately made as the extent of the breach must be put in context of the risk.

As a minimum, the communication to the affected users will include a description of how and when the breach occurred and what data was involved. We will also include details of what has already been done to respond to the risks posed by the breach. Any suggested steps that the user can take to further protect themselves following the breach will also be communicated.

**3.4 Evaluation and response**

Once the breach has been fully understood and contained, it is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it.

If the breach was caused, even in part, by systemic and on-going problems, then simply containing the breach and continuing ‘business as usual’ is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

The following points will be considered within the review process:

 Make sure NFA fully understand how the personal data is acquired, processed, and where and how it is stored. This covers manual processes as well as within electronic systems.

 Establish where the biggest risks lie. For example, how much sensitive personal data do NFA hold?

 Risks will arise when sharing with or disclosing to others – both within NFA, partners and customers. We must ensure that not only the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.

 Identify weak points in our existing security measures such as the use of portable storage devices or access to public networks.

 Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

**4 Definitions**

**4.1 Data Controller**

A person who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**4.2 Data Subject**

Any living individual who is the subject of the personal data.

**4.3 Data Processor**

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**4.4 Personal data**

Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. As well as including obviously personal data such as names and addresses (including e-mail addresses), the definition includes ‘any expression of opinion about the individual and any indication of the intentions of the Data Controller … in respect of the individual’. The definition is therefore quite broad, and may cover information such as an individual’s health, beliefs, personal hobbies, or business activities, for example.

**4.5 Sensitive Personal data**

Sensitive personal data means personal data consisting of information as to –

(a) the racial or ethnic origin of the data subject,

(b) political opinions,

(c) religious beliefs or other beliefs of a similar nature,

(d) whether the person is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) physical or mental health or condition,

(f) sexual life,

(g) the commission or alleged commission by the person of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings.

**4.6 Recipient**

Anyone who receives personal data, except the Data Controller, Data Subject, or Data Processor.

**4.7 Third Party**

Third party, in relation to personal data, means any person other than –

(i) the data subject,

(j) the data controller, or

(k) any data processor or other person authorised to process data for the data controller or processor.

**4.8 Processing**

Processing is defined as including but not limited to collection, storage, use, disclosure, or destruction of personal data.