**NEW HOPE DATA PROTECTION POLICY**

**INTRODUCTION**

This Data Protection Policy forms the bedrock of New Hope’s Information Governance Framework. New Hope is fully committed to compliance with the requirements of the Data Protection Act 1998 (DPA 1998). This policy takes into account the new regulations coming into force on 25th May 2018, namely the General Data Protection Regulations (GDPR). The emphasis under GDPR is on “Privacy by Design”. Data privacy at New Hope should be the default, not an afterthought. Consent for use of personal data will now be strictly “opt in”, so there will be no more “tick this box if you *don’t want…..”.*”Tick this box if you DO want…..” becomes the norm. New Hope will seek written permission from parents/carers/staff/third parties to hold all information and only keep information necessary by law e.g. Ofsted Regulations and safety checks re staff (DBS) . New Hope WILL NOT use any forms of mailing lists.

**Policy Statement.**

New Hope directors/trustees take overall responsibility and accountability for compliance with the Data Protection Act 1998 and the new rules GDPR. Discharging these responsibilities through the implementation of this policy will mean that New Hope approaches the processing of personal data in an effective and efficient manner. This policy sets the benchmark for how data is captured, handled, stored, shared and disposed of. It recognises that our integrity is key to our customers’ willingness to share what is always sensitive personal information. It promotes confidentiality and security for personal data.

**Objectives.**

The objectives of this policy are to:

* Understand the principles and rights detailed in the Data Protection Act 1998;
* Recognise and understand the difference between personal data and sensitive data;
* Ensure that adequate procedures and protections are in place to lawfully fulfil and meet all these requirements;
* Recognise the need to share data with other organisations and to ensure adequate procedures and protocols are in place;
* Recognise and detail those exemptions to the Data Protection Act and ensure adequate procedures and guidance are available to lawfully work with those exemptions;
* Make clear to New Hope’s employees and relevant parties the risks to be managed with regards to confidentiality, storage and disposal of data and the consequences of failure;

**Legalisation and Regulation.**

* Data Protection Act 1998 (the DPA)
* European Data Protection Directive 95/46/EC
* The DPA is enforced and regulated by the Information Commissioner acting through the Information Commissioner’s Office.

**Performance Standards and Performance Indicators.**

* Staff to read this policy and sign to say they understand it and are aware of breaches of confidentiality as it relates to the Data Protection Policy.
* Managers to have a “clear desk” policy.
* Staff to receive “in house” training regarding the importance of Data Protection privacy

**Policy Scope**

The policy applies to all personal data that New Hope holds relating to identifiable individuals. Personal data can include but is not limited to:

Names,

Addresses,

Contact Details;

Personal diversity Information including age, gender, ethnicity, disability, sexuality, religion, trade union membership, criminal records and financial information; Types of individuals that personal data is held on includes but is not limited to:

* Current, prospective and former employees, customer and trustees/directors,

In addition, we are required by law to collect and / or process children’s information to comply with Ofsted regulations. We are also required by Ofsted to hold employees DBS reference numbers.

**Roles and Responsibilities**

New Hope’s directors/trustees and its designated officers have overall responsibility for the implementation of this policy. Directors/Trustees will:

* Set the tone and influence the culture of data protection for the organisation
* Ensure that they are adequately trained and compliant within the principles of the DPA/GDPR regulations and New Hope’s procedures when processing personal data;
* Approve and promote the Data Protection Policy and other relevant policies in the Information Governance Framework;
* Actively participate in the management of any significant data protection breach;
* Management will lead by example in setting the tone and culture for how data is implemented;
* Always consider the personal Privacy Impacts implications for any existing and future service development;
* Senior management are responsible for ensuring that their staff implement the policy on the ground and that any training opportunities, audits, investigations and policy development is fully engaged with.
* Ensure security of data
* Control access to data
* Data back ups

**Staff**

Staff who process personal data on a regular basis will have an understanding of, adhere to, the data management principles and practices within their remit. The data protection policy will be incorporated into the employee induction process including a disclaimer stating that the policy has been read and understood. Where there are concerns that the principles of the Act may be being breached they have a responsibility to notify New Hope managers/trustees immediately in order that it may be rectified.

Managers are responsible for ensuring that the Policy is up to date, fit for purpose and being followed by the business.

**The Principles of data protection.**

The Information Commissioner who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with eight data protection principles of “good information handling.”

The eight Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. 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.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under the Data Protection Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

**Specific Conditions to fair and lawful processing.**

We will ensure that at least one of the following conditions are met before we process any personal data:

The individual has consented to the processing

The processing is necessary for the performance of a contract with the individual

The processing is required under a legal obligation (other than one imposed by a contract)

The processing is necessary to protect vital interests of the individual

The processing is necessary to carry out public functions e.g. Administration of justice

The processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual)

Under the Act, one of a set of additional conditions must be met for “sensitive personal data”. This includes information about racial or ethnic origin, political opinions, religious and other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions. We will ensure that one of the following additional conditions are met before we process any sensitive personal data:

* The individual has explicitly consented to the processing;
* We are required by law to process the information for employment purposes;
* We need to process the information in order to protect the vital interests of the individual or another person; or,
* The processing is necessary to deal with the administration of justice or legal proceedings.

**Personal and Sensitive Personal Data**

The Data Protection Act provides conditions for the processing of any personal data. It also makes a distinction between personal data, and ‘Sensitive’ personal data. ‘Sensitive’ personal data will be subject to additional access security levels and collected only with the expressed consent of the data subject. Personal data is defined as data relating to a living individual who can be indemnified from:

* That data.
* That data, and other information which is in possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive Personal data consists of the following information as to:

* The racial or ethnic origin of the data subject;
* Their political opinions;
* Their religious beliefs or other beliefs of a similar nature;
* Trade union membership;
* Physical or mental health condition;
* Sexual orientation;
* Criminal proceedings or convictions.

**Transgender Data Subjects holding a Gender Recognition Certificate**

Section 22 of the Gender Recognition Act 2004 establishes that it is an offence for a person to disclose information acquired in an official capacity about a person’s application for a gender recognition certificate or about the gender history of a successful applicant. Additional procedural security will be put in place to ensure this.

**The rights of data subjects**

In addition to the rights detailed below, all staff, data subjects and other users are entitled to know:

* Know what information New Hope holds and processes about them and why;
* Know how to gain access to it;
* Know how to keep it up to date;
* Know who it will be shared with and why;
* Know what New Hope is doing to comply with its obligations under the 1998 Act and the GDPR regulations coming into force in May 2018

New Hope will clearly spell out the rights and reasons for processing individual’s personal data in the respective privacy notice for any paper or online form.

**Access to personal data.**

Data subjects may request by writing to the manager details of the information that is held about them and the purpose(s) for which it is held. New Hope will provide the information in a permanent form as held at the time of the request. The request will be met within 40 calendar days of receiving the request, or later, of receipt of any supplementary information needed to establish the data subject’s relationship with New Hope or verify their identity. This is also subject to New Hope obtaining the £10 administration fee.

**Right to prevent distress**

Data subjects are entitled, by notice in writing to require us to cease (or not to begin) processing personal data on the grounds that it is causing or is likely to cause substantial damage or distress to them or to another and that damage or distress is or would be unwarranted. This does not apply where they have consented to the processing, the processing is necessary for compliance with a legal obligation, or the processing is necessary to protect their vital interests.

**Right to prevent direct marketing**

Data subjects are entitled, by notice in writing, to require us to stop using information about them for the purposes of direct marketing, direct marketing means the communication (by whatever means) of any advertising or marketing material which is directed at them. Under GDPR regulations New Hope will seek to gain written consent from staff/customers/third parties to receive marketing messages. New Hope shall not sell, rent, distribute or otherwise make user data commercially available to any third party, except as described in ‘exemptions’ (below) or with expressed prior permission from the individual.

**Right to prevent automated decision taking**

Data subjects are entitled, by notice in writing, to require us to ensure that no decision taken by or on behalf of us and which significantly affects them based solely on the automated processing of their information.

**Right to compensation**

Data subjects are entitled to take action to seek compensation if they can prove damage or distress occurred as a direct result of any contravention of the data Protection Act by New Hope.

**Right to correction.**

Data subjects are entitled to request action to rectify, erase or destroy inaccurate data.

**Data Sharing**

Any data sharing, with the exception of the exemptions below, will be carried out under a written information sharing protocol, agreement or contract. The protocol, contract or agreement will set out the scope and limits of the sharing. Copies of each active Information Sharing Agreement will be centrally recorded and made available on our web site.

**Exemptions**

There are a number of exemptions from, and modifications to, various provisions of the Act, whereby New Hope may be required to disclose personal data about data subjects without their consent. These include: -

* These include, but are not limited to, requests for disclosure to police and other statutory organisations for the purposes of:
* The prevention or detection of crime;
* The detection of fraud;
* The collection of Council Tax;
* In connection with court proceedings.

**Sanctions for non-compliance**

There are a number of tools available to the Information Commissioner’s Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller currently up to the value of £500,000. Under the new GDPR regulations coming into force on May 25th 2018 the Information Commissioner’s Office can, in worst case scenario attract a fine of 4% of annual revenue or 20m Euros which ever is the greater. Even a relatively modest breach could cost tens of thousands of pounds. This policy ensures New Hope is compliant with the new regulations.

**Adopting the EU Data Protection Regulation. (GDPR REGULATIONS)**

The EU Protection Regulation represents a significant change and aims to bring a common and consistent approach across all 27 EU states. Another aim is to make the regulations fit for dealing with data protection and security in the modern era. Significant changes that are already being actioned by New Hope include:

* Have a central register of readily accessible up to date policies, procedures and documentation;
* Appoint a dedicated Data Protection Officer
* Enhance incident management processes and breach notification processes to detect and respond immediately;
* Review data classification, retention, collection, destruction, storage and search covering all modern data collection sources in preparation for ‘the right to be forgotten’, ‘right to erasure’, ‘privacy by design’ and the ‘right to data portability’.
* New Hope will seek written permission from employees to hold necessary information regarding their suitability to work at New Hope (we are required to hold this information under Ofsted regulations for example DBS checks and training records)
* New Hope will seek written permission from parents are carers to hold necessary information about their children (we are required to hold children’s information under Ofsted regulations and keep these records for a specified time period of 21 years and 8 months)
* New Hope will seek written permission from parents and carers to hold their e mail addresses.
* All unnecessary information will be removed from New Hope both in paper form and electronically.
* New Hope will keep all passwords for computers stored in a locked filing cabinet in a locked office. Only 4 staff members will have access to any data relating to New Hope, its employees or its customers.
* All new staff and customers will have access to this policy: it will be displayed on our web site.

**Equality and Diversity**

New Hope is committed to developing an organisational culture which values people from all sections of the community and the contribution each individual can make to our work. This means that we value each individual in their own right, regardless of whether or not they belong to any particular section of society.

New Hope will ensure this policy is applied fairly and consistently to all customers, employees and other stakeholders. We will not directly or indirectly discriminate against any person or group of people and when applying this policy, we will act sensitively towards the diverse needs of individuals and communities.

**Monitoring**

Compliance with the Data Protection Act and this policy will be monitored by the Data Protection Officer every six months.

**Review**

This policy will be reviewed every year or when significant legislative changes come into force whichever is sooner. Procedural amendments will be carried out when required by the business.

**Glossary of Terms**

**Data**

Any recorded information held by New Hope and from which a living individual can be identified be this on paper or electronically.

**Data Processing**

Any activity/operation performed on personal data – whether held – electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending, and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. It is difficult to envisage any activity which does not amount to processing.

**Sensitive Personal Data**

Information relating to an individual’s race/ethnic origin, their political opinions, religion, trade union membership, health, sexual life, criminal or alleged offences.

**Updated January 2019**

**Review Date February 2020.**