ThinkForward
Successful school to work transitions

IT SECURITY AND DATA PROTECTION POLICY

Document History

Date	Version	Description	Approved	Owner
Jun 2018	V1		Ben Haber	Performance & Operations
June 2020	V2	Review and refresh roles, description of process and ensure compliant with current practice	Vicki Wright, COO	Operations
July 2020	V3	Review by external legal counsel		

Contents

1. Who Does This Policy Apply To?

In order to deliver the ThinkForward programme, ThinkForward and its directors and employees may collect, store and process personal data about current, past and prospective young persons, school contacts, volunteers and others with whom we engage.

This policy sets out ThinkForward's approach to protecting personal data and applies to all information, information systems, networks, applications, locations and users of the personal data collected by ThinkForward, whether such users are directly employed by ThinkForward or operating under the terms of a sub-contract arrangement with ThinkForward. All such users must read, understand and comply with the terms of this policy. It provides essential information concerning your engagement with ThinkForward but does not form part of your contract of employment or contract for the provision of services (as applicable). Compliance with this policy by all staff, as amended from time to time, is mandatory. For further details about how employee data is collected and processed by ThinkForward, please see the Employee Data Protection Statement.

This policy has been approved by the Executive Team and any breach will be taken seriously and may result in disciplinary action being taken. Any individual who considers that this policy has not been followed should raise the matter with their line manager or in the case of contractors, the person to whom they report.

2. Responsibilities

Responsibility for implementing this policy is delegated through the line management structure to operational managers.

It is each individual's responsibility to ensure they are aware of, and comply with, their responsibilities and duties under this policy, and to have them explained if in doubt. This policy will be reviewed from time to time and may be varied, amended or revoked, in whole or in part, at any time. Changes will be effected by way of individual notice or notice to all staff.

Information security risks shall be recorded within a risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals by the COO and subsequently by the Board of Trustees.

3. Principles

The type of personal data that ThinkForward may process includes, but is not limited to, information about: current, past and prospective employees or contractors; beneficiaries on the ThinkForward programme; past, current and prospective funders (for more details see Section 7.3); suppliers and others with whom it communicates. This could include:

- General personal data, including names, dates of birth, gender and contact details.
- Information necessary for ThinkForward to comply with its legal and regulatory obligations, including ThinkForward's safeguarding procedures.
- Data regarding an individual's interactions with ThinkForward, including details of calls, emails, classes, sessions, meetings and events attended with ThinkForward.
- Personal data in respect of those attending programmes delivered by ThinkForward,

including contact details and information about their personal circumstances relevant to their involvement with ThinkForward gathered from their school/education provider, for example about their behaviour and attendance.

ThinkForward may also process sensitive personal data in accordance with section 7 below, which may include an individual's health data, data relating to ethnicity or information relating to an individual's commission or alleged commission (and/or any related proceedings) of a criminal offence.

This policy is based on principles which:

- Ensure that personal data is collected and processed by ThinkForward in accordance with relevant data protection legislation.
- Ensure the availability of data and processing resources.
- Provide assurance for the confidentiality and integrity of this data.
- Ensure the integrity of information assets and protect them from unauthorised use.
- Ensure the confidentiality of processed data, and prevent unauthorised disclosure or use.
- Ensure the integrity of processed data, and prevent the unauthorised and undetected modification, substitution, insertion, and deletion of that data.

ThinkForward fully endorses the six data protection principles of the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") (together with the UK Data Protection Act 2018 and any other law implemented in the UK in respect of data protection, collectively the "**Data Protection Legislation**"). ThinkForward recognises the importance of the correct and lawful treatment of personal data; not handling information in a proper and secure manner can lead to real harm and distress to the person that the information relates to, and can cause harm to ThinkForward's reputation. We aim to ensure that personal data is processed in accordance with the following principles set out in the GDPR:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. What is Data Protection and what are ThinkForward's legal responsibilities?

ThinkForward has a responsibility to abide by all relevant UK and, throughout the transition period following the UK's exit from the EU, all European Union legislation and may be held accountable for any breaches of information security for which they may be held responsible. Staff will be made aware of their responsibility to comply with current legislation and any new relevant legislation as it is implemented. Data protection laws consist of rules that are designed to:

- safeguard the handling and use of personal information;
- respect a person's rights over his/her personal information; and
- enable organisations like ThinkForward to legitimately use personal information to operate its business.

Personal data, whether it is held on paper, on computer or in another form, will be subject to the appropriate legal safeguards as specified in the Data Protection Legislation.
ThinkForward will also operate in accordance with standards set out in contracts and ultimately with ISO27001.

5. Definitions

5.1 **Information Asset**

An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to ThinkForward.

5.2 **Processing**

Data protection law applies where there is processing of personal data which means any use of the personal data on behalf of ThinkForward including but not limited to collecting, holding or transferring the data, or accessing the data, whether the data is accessed from inside or outside of the UK.

5.3 **Personal data**

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
'Personal data' includes both facts and opinions about an individual.
Information may be personal data even if the individual will only be identifiable when the information is tied to other data held by ThinkForward or other data that it is likely ThinkForward will hold. So, for example, a telephone number on its own may be personal data if an individual can be identified from that number through a database which links that number to a name. Each individual to whom the information relates to is known as a "data subject".

5.4 Sensitive personal data

Sensitive personal data is known as "special category data" which is defined in the Data Protection Legislation to include information as to -

a) the racial or ethnic origin of the data subject,
b) his or her political opinions,
c) his or her religious beliefs or other beliefs of a similar nature,
d) whether he or she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) his or her physical or mental health or condition,
f) his or her sexual life or orientation,
g) the commission or alleged commission by him or her of any offence, or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings, and
h) his or her genetic or biometric data.

5.5 Information security events

An information security event indicates that the security of an information system, service, or network may have been breached or compromised.

6. Control and access to assets

6.1 Security Control of Assets

Each Information Asset shall have a named custodian who shall be responsible for the information security of that asset. All assets will be recorded on an asset register, maintained by the Data and Insight Executive.

6.2 Access Controls

Only authorised personnel, who have a justified and agreed business need, shall be given access to Information Assets. Access to information and computer facilities shall be restricted to authorised users, and all staff are responsible for ensuring that any doubt about a person's authorisation to be in the workplace is reported. Authorisation to use an application will be granted by the COO or delegated authority on a business need only following a request from the appropriate team leader. Individual members of Staff will not be able to make such requests directly.

Access to equipment and data held by ThinkForward will be removed from individuals when they leave the organisation. The team leader will be responsible for ensuring all equipment and resources owned by ThinkForward are returned by each individual prior to leaving the organisation.

Personal information must not be disclosed either orally or in writing or otherwise to any unauthorised third party. See the IT and Phones policy for guidance on passwords.

6.3 Clear desk and screen policy

Employees must maintain a clear desk and computer screens when they are absent from their normal desk and outside normal working hours. Desks, lockers and filing cabinets should be kept locked if they hold confidential information of any kind.

In addition, screens on which sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. All staff should log off from their PC, or lock their screen, when it is left unattended.

6.4 Protection from Malicious Software

ThinkForward shall use software countermeasures to protect itself against the threat of malicious software. Users must not install software on ThinkForward property; users found breaching this requirement will be subject to disciplinary procedures.

6.5 IT systems

ThinkForward shall ensure that all new information systems, applications and networks include security attributes that are approved by the COO or the Board of Trustees and tested by the operations team before they commence operation. Changes to information systems, applications or networks shall be reviewed and approved by the COO. All changes will be recorded.

6.6 Equipment security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. All protection will be authorised by the COO. Individual members of staff to whom equipment is issued are personally responsible for its safekeeping and ensuring authorised access only.

Where equipment is installed and maintained at a single location, the team leader will be responsible for the security of equipment. Any loss or damage to equipment must be reported via the line Manager to the HR & Operations Manager immediately.

ThinkForward's Business Continuity Plan shall outline the detail for recovering all critical information, applications, systems and networks in the event of major disruption (e.g. fire, flood, major power outages).

6.7 Protecting data taken off-site

Files or equipment containing sensitive data (which shall include personal data, financial data relating to ThinkForward (whether P&L or balance sheet and whether actual or budget, which is not already filed at Companies House, the Charity Commission or the Office of the Scottish Charities Regulator) and data which contains, in whole or in part, any bids or funding applications, any contracts with funders or other third parties and/or any document listing or summarising contracts held) shall not be left unattended at any time or in any place where unauthorised persons might gain access to them. They should be transported securely. Other mobile devices should be security coded to prevent unauthorised access.

ThinkForward will endeavour to ensure that, when sensitive personal data is sent by email, the sensitive personal data shall be encrypted or password protected so as to prevent unauthorised access.

6.8 Encryption

Encryption is used for both electronic storage and electronic transfer of personal data.

All personal data which is stored or used in any mobile electronic data system, including (but not limited to) laptops, memory sticks, mobile phones, PDAs, CD-R, CD-R/W (and the DVD versions), portable hard drives etc, will be encrypted. Requests to store personal data in a plain format must be approved by the Data Protection Lead. All encryption materials and products

used are approved by the COO. Users breaching this requirement will be subject to disciplinary procedures.

6.9 Emailing

ThinkForward staff including delivery partners will endeavour to ensure that, when sensitive personal is sent by email, the sensitive personal data shall be encrypted or password protected. ThinkForward retains the right to send its own data using email. This extends to:

- Discussing general ThinkForward programme aims, partnerships, meetings, activities documents, staff or systems, including but not limited to schools funded by government grants
- Discussing general outcomes – i.e. aggregated improvements in pupil behaviour and attainment as defined by ThinkForward, including but not limited to outcomes also measured for government grants
- Discussing performance against contracts between ThinkForward and other parties including government grants

7. Processing of personal and sensitive personal data

ThinkForward will not process personal data unless at least one of the following conditions are met:

- (a) Consent: the individual has given clear consent for ThinkForward to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract ThinkForward has with the individual, or because they have asked ThinkForward to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for ThinkForward to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for ThinkForward to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for legitimate interests pursued by ThinkForward or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

7.1 Processing Personal Data

As part of our obligation to process fairly, ThinkForward must ensure that it can justify the reasons for collecting and processing personal data. In most circumstances, ThinkForward would expect to be able to justify processing the personal data on the basis of one or more of the following conditions (which are set out in the Data Protection Legislation):

a) the relevant individual has expressly consented to ThinkForward making use of their personal data;
b) it is necessary for ThinkForward to comply with its legal obligations;
c) it is necessary for ThinkForward to pursue a legitimate business interest; and/or
d) it is necessary for the performance of a contract with the individual.

7.2 Processing Sensitive Personal Data

Particular care should be taken in respect of sensitive personal data that is collected. ThinkForward's duty of care is higher under the Data Protection Legislation in respect of sensitive personal data, and it is also ThinkForward's internal policy to use higher levels of security in respect of this information due to the harm that may be suffered if such information were lost/misused.

Under the GDPR, the processing of sensitive personal data is only permissible where an additional basis set out in Article 9 of the GDPR is met. In most cases, we would expect to be able to justify processing the sensitive personal data on the basis that the individual has given their explicit and informed consent to our making use of their sensitive personal data.

7.3 Processing of Personal Data - Funders and Supporters

We only ever collect information on current and potential funders and supporters if at least one of the following conditions are met:

- We have their explicit consent
- It is necessary to collect the information in order to deliver a contract with the individual
- The information is required under a legal obligation
- The information is necessary to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual)

Information that we collect on current and potential funders and supporters includes:

- Contact information
- Information on past grants or investments given to ThinkForward and other organisations
- Interactions with ThinkForward, including details on calls, emails, meetings and events attended with ThinkForward

Funders and supporters should understand that they have the right to request a copy of the information that we hold about them. If they would like a copy of some or all of their personal information, they can request this via email. We want to make sure that their personal information is accurate and up to date. They may ask us to correct or remove information they think is inaccurate.

7.4 Keeping Personal Data Secure

As staff of ThinkForward, you must ensure that the personal data under your control cannot be removed or copied without your knowledge or permission or accessed by an unauthorised person. You must ensure that you follow the safeguards set out at section 6 above in respect of personal data.

Access to sensitive personal data should be strictly controlled and all such sensitive personal data should be saved securely in: a password protected database; a separate, access-limited folder; or otherwise in a secure or locked environment with access only granted where strictly necessary. ThinkForward will keep as little sensitive personal data as possible and only where

necessary. Examples of when sensitive personal data is collected and processed include without limitation (a) to monitor ThinkForward's compliance with equality and diversity requirements; (b) where necessary to monitor a young person's mental health as part of the coaching programme; and (c) where it is needed to complete appropriate background checks or to act on instructions from the police or local authorities.

Access to any sensitive personal data should be limited to only those ThinkForward personnel who strictly need to be aware of the information.

7.5 Retention of personal data

You should ensure that the personal data for which you are responsible is kept up to date, is accurate and is deleted when it is no longer required. Without regular updates, there is an increased risk that outdated personal data will be used by ThinkForward in error. Unless you have been informed otherwise by the Data Protection Lead all personal data must be properly disposed of at the end of its specified retention periods (see Schedule 1 below). To ensure the security of personal data it is important that you follow the steps below when disposing of such information. These steps should also be followed to delete personal data where an individual has appropriately exercised their rights to erasure (see section 13).

Data on past ThinkForward beneficiaries, funders and supporters is stored (and may be archived) for six years following end of the programme in which they participated. All staff are responsible for ensuring that information is not kept for longer than necessary and is destroyed or erased when no longer required.

7.5.1 Soft copy deletion

Where personal data is held electronically (e.g. on hard drives, USBs, DVDs and other storage media) it will need to be deleted at the end of the relevant retention period. However, simply deleting the personal data may not be sufficient since it may still be accessible either on the device until it is overwritten by a new file or in our system back-ups. You should be diligent to ensure personal data is fully deleted on your device and check with the Data Protection Lead that it has been removed from ThinkForward's central systems.

7.5.2 Hard copy disposal

You should regularly review the paper records that you hold and safely and securely dispose of these records where you no longer need to make use of the relevant personal data. Check with the Data Protection Lead if you are unsure on how to do this safely and securely.

7.6 Sharing Personal Data

In carrying out ThinkForward's activities we will be required from time to time to share certain personal data we hold with third parties. Where we transfer any personal data to third parties, it is important to be satisfied that (i) we are justified in doing so and (ii) each such third party has

the appropriate technical and organisational measures in place to ensure the security of the personal data.

Where you have the right to share personal data, you should ensure that a written contract is put in place with the third-party recipient before they are granted access to the data. This contract must comply with the Data Protection Legislation and so it is important that it is reviewed by the Data Protection Lead.

Personal data should not be transferred outside of the UK unless ThinkForward is satisfied that the recipient of the personal data has appropriate measures in place to ensure its security. Note that if the recipient of the personal data is situated outside of UK it may be necessary to comply with additional requirements under the Data Protection Legislation to ensure the security of the personal data.

8. Information security events and weaknesses

A data breach or breach of security could involve a malicious third party hacker or "phishing" attack, or could be something as simple as a laptop being left on a train or login details falling into the wrong hands. ThinkForward may have an obligation to inform the data protection regulator, the UK's Information Commissioner's Office (and in some cases affected individuals) in the event that it has suffered a breach within 72 hours of becoming aware of the personal data breach.

Any member of staff or sub-contractors who have information regarding a data breach, breach of security or suspect weaknesses in the system must report the details immediately to their Line Manager and ultimately to the COO. Incidents must also be reported as required under the terms of contracts or Service Level Agreements with third parties. All incidents shall be investigated to establish their cause and impacts with a view to avoiding similar events. A report of all such incidents will be monitored by the COO and any action resulting from such incidents will be agreed by the Executive Team.

8.1 Reporting

The COO shall keep the Executive Team informed of the information security status of the organisation by means of regular reports and presentations. The COO will report to the Board of Trustees any breach of security likely to have an impact on business continuity or the organisation’s financial status.

9. Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability as set out in sections 10 to 16 below. We must ensure individuals can exercise their rights in the following ways:

9.1 Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

9.2 Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

9.3 Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than within one month. This can be extended to two months with permission from the Data Protection Lead.

9.4 Right to erasure

- We must delete or remove an individual's data if requested and there is no legal ground for its continued processing.

9.5 Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data if there is no longer a legal ground for us to do so.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

9.6 Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

9.7 Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

9.8 Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

10. Subject Access

An individual has the right under the Data Protection Legislation to submit a subject access request ("**SAR**") and to receive (i) confirmation that their personal data is being processed, (ii) a

description of the relevant data held by ThinkForward, (iii) a summary of the purposes for which the data is being processed, (iv) where possible, for how long ThinkForward intends to keep the information, (v) details of any organisation to whom that information is being, or might be disclosed and (vi) a copy of the relevant data.

A SAR does not need to be received as a formal request or include the words "subject access request" and there are very few rules on how to make a SAR. A SAR can be made verbally or in writing (including email) but should include sufficient information to identify the requesting person to ThinkForward's satisfaction. If more information is needed to verify the requesting person, we should write to that person requesting further identifying information (e.g. copies of their passport/driving licence).

11. How we deal with subject access requests

We must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt of the SAR. In some instances where responding to the request is particularly complex and time-consuming it may be possible to extend the deadline to two months from receipt of the SAR. If extending the deadline, the individual should be informed. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the Data Protection Lead .

If you receive what you think is or may be a SAR, please notify the COO as soon as possible and send details of the SAR to info@thinkforward.org.uk.

12. Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than within one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and we must receive express permission from the Data Protection Lead first.

13. Right to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances (and where ThinkForward no longer has an alternative legal ground for holding the data):

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn

- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child under the age of 13

14. How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

15. The right to object

Individuals have the right to object to their data being used on grounds relating to their situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

16. The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

17. Staff Responsibilities

All staff are responsible for:

- checking that any personal data that they provide to ThinkForward is accurate and up to date;
- informing ThinkForward of any changes to information which they have provided, e.g. changes of address; and
- checking any information that ThinkForward may send out from time to time, giving details of information that is being kept and processed.

If, as part of their involvement with ThinkForward, staff collect information about other people (e.g. about personal circumstances, or about other staff who work for ThinkForward), they must comply with this policy for holding and maintaining the data that they collect.

18. Publication of Charity Information

Information published as a part of journalistic material is exempt from data protection laws. This includes, for example, information about staff contained within externally circulated publications such as the ThinkForward diary. Any individual who wishes for information concerning themselves to be excluded from ThinkForward publications should immediately inform the person whom they report to.

19. Training

ThinkForward will ensure that all ThinkForward staff, where relevant, and in any event as part of the induction process, undergo training in relation to data protection issues. If you feel you require additional or refresher training, please contact the COO, who is also the Data Protection Lead.

20. Review and Evaluation of this Policy

ThinkForward will periodically review the implementation of this Data Protection Policy in respect of its suitability, adequacy and effectiveness and is committed to making improvements where appropriate.

Schedule 1

Data Retention Schedule

Below is a table setting out the suggested retention periods for the types of personal data that ThinkForward holds:

Type of Data	Retention Period
Beneficiaries of the ThinkForward programme	
Personal data e.g. name, email, school	6 years after the end of the programme
Case Notes/Meeting records	6 years after the end of the programme
Safeguarding Reports/Referrals	6 years after the end of the programme or as long as required by the police or local authority.
Parental contact details	6 years after the end of the programme
Evidence supporting an outcomes claim	6 years after the successful claim date or as long as reasonably required by the funder
Beneficiaries of the MoveForward programme	
Personal data e.g. name, email, school	6 years after exiting the programme
Case Notes/Meeting records	6 years after exiting the programme
Safeguarding Reports/Referrals	6 years after exiting the programme or as long as required by the police or local authority.
Parental contact details	6 years after exiting the programme
Evidence supporting an outcomes claim	6 years after the successful claim date or as long as reasonably required by the funder
Staff	
Personnel files	6 years after employment with ThinkForward ceases
Recruitment data and interview notes (for unsuccessful candidates)	7 months after an appointment is made
Safeguarding Reports/Referrals	6 years after the end of the programme or as long as required by the police or local authority.
Payroll Data	6 years after the end of the tax year to which they relate
Funders	
Contact details	As long as the individual is a contact of ThinkForward. Information should be deleted within 6 months of the individual indicating they no longer wish to be contacted by ThinkForward in respect of potential partnership opportunities.
Details of interactions with ThinkForward	As long as necessary for the purposes of the individual's engagement with ThinkForward.
Gift Aid Claims	6 years from the end of the tax year of the claim
Contractors/suppliers	
Name and contact details	As long as necessary for the purposes of the individual's engagement with ThinkForward.

Details of interactions with ThinkForward	As long as necessary for the purposes of the individual's engagement with ThinkForward.
Other	
Names/Emails of school contacts	As long as the individual is a contact for ThinkForward. Information should be deleted within 6 months of a change in contact.
Names and contact details of volunteers	6 years after their final volunteering engagement
Trustee meeting minutes (these may contain personal data dependent upon issues arising	At least 10 years