path
YORKSHIRE

Preparing communities for the world of work

Policies Handbook

PATH (Yorkshire) Limited
29 Harrogate Road
Chapel Allerton
Leeds LS7 3PD

Contents

Page

Anti-bribery and Anti-corruption Policy	02
Data Protection Policy	09
Health & Safety Policy	25
Diversity, Equality and Inclusion	30
Whistleblowing Policy	37
Safeguarding Policy	43
Customer-Learner Complaints Procedure	47
Secure Disposal of IT Equipment and Information	49
Appendix 1	56
Version Control	58
Statutory Guidance	58

Anti-bribery and anti-corruption policy

1. Policy statement

1.1 We conduct all our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery and corruption.

1.2 We take our legal responsibilities very seriously. We will uphold all laws relevant to countering bribery and corruption [in all the jurisdictions in which we operate]. However, we remain bound by UK laws, including the Bribery Act 2010, in respect of our conduct both at home and abroad.

2. About this policy

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for and on our behalf, in observing and upholding our position on bribery and corruption; and

(b) provide information and guidance to those working for and on our behalf on how to recognise and deal with bribery and corruption issues.

(c) This policy has been agreed and implement with the PATH Yorkshire Board of Trustees

(d) This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

3. Who does this policy apply to?

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located.

4. Who is responsible for the policy?

4.1 The **PATH Yorkshire Board of Trustees** has overall responsibility for the effective operation of this policy but has delegated responsibility for overseeing its implementation to CEO. Suggestions for change should be reported to the CEO.

4.2 Line managers have day-to-day responsibility for this policy and you should refer any questions about this policy to them in the first instance. They will involve the CEO where appropriate.

4.3 This policy is reviewed continually by the CEO [in consultation with **the PATH Yorkshire Board of Trustees**.

5. Definitions

5.1 Bribery **is offering, promising, giving, or accepting any financial or other advantage, to induce** the recipient or any other person to act improperly in the performance of their functions, or to reward them for acting improperly, or where the recipient would act improperly by accepting the advantage.

5.2 An **advantage** includes money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or anything else of value.

5.3 A person acts **improperly** where they act illegally, unethically, or contrary to an expectation of good faith or impartiality, or where they abuse a position of trust. The improper acts may be in relation to any business or professional activities, public functions, acts in the course of employment, or other activities by or on behalf of any organisation of any kind.

5.4 It is a criminal offence to offer, promise, give, request, or accept a bribe. Individuals found guilty can be punished by up to ten years' imprisonment and/or a fine and employers that fail to prevent bribery can face an unlimited fine, exclusion from tendering for public contracts, and damage to its reputation.

5.5 **Corruption** is the abuse of entrusted power or position for private gain.

Examples:

Offering a bribe: You offer a potential client tickets to a major sporting event, but only if they agree to do business with us.

This would be an offence as you are making the offer to gain a commercial and contractual advantage. We may also be found to have committed an offence because the offer has been made to obtain business for us. It may also be an offence for the potential client to accept your offer.

Receiving a bribe: A supplier gives your nephew a job, but makes it clear that in return they expect you to use your influence in our organisation to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

Bribing a foreign official: You arrange for the business to pay an additional "facilitation" payment to a foreign official to speed up an administrative process, such as clearing our goods through customs.

The offence of bribing a foreign public official is committed as soon as the offer is made. This is because it is made to gain a business advantage for us. We may also be found to have committed an offence.

5.6 Facilitation payments, also known as "back-handers" or "grease payments", are typically small, unofficial payments made to secure or expedite a routine or necessary action (for example, by a government official). They are not common in the UK, but are common in some other jurisdictions [in which we operate].

5.7 Kickbacks are typically payments made in return for a business favour or advantage.

5.8 Third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

6. What you must not do

6.1 It is not acceptable for you (or someone on your behalf) to:

(a) give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;

(b) give or accept a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome;

(c) accept a payment, gift or hospitality from a third party that you know or suspect is offered with the expectation that it will provide a business advantage for them or anyone else in return;

(d) offer or accept a gift to or from government officials or representatives, or politicians or political parties[, without the prior approval of the PATH Yorkshire Board of Trustees.

(e) threaten or retaliate against another individual who has refused to commit a bribery offence or who has raised concerns under this policy; or

(f) engage in any other activity that might lead to a breach of this policy.

(g) Facilitation payments and kickbacks

6.2 We do not make, and will not accept, facilitation payments or "kickbacks" of any kind. See clause 5 for definitions of these terms.

6.3 You must avoid any activity that might lead to a facilitation payment or kickback being made or accepted by us or on our behalf, or that might suggest that such a payment will be made or accepted. If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt which details the reason for the payment. If you have any suspicions, concerns or queries regarding a payment, you should raise these with the Compliance Manager.

7. Gifts, hospitality and expenses

7.1 This policy allows reasonable and appropriate hospitality or entertainment given to or received from third parties, for the purposes of:

(a) establishing or maintaining good business relationships;

(b) improving or maintaining our image or reputation; or

(c) marketing or presenting our products and/or services effectively.

(d) [You are prohibited from [accepting a gift from or] giving a gift to a third party OR The giving [and accepting] of gifts is allowed if the following requirements are met:

(e) it is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits;

(f) it is given in our name, not in your name;

(g) it does not include cash or a cash equivalent (such as gift certificates or vouchers);

(h) it is appropriate in the circumstances, taking account of the reason for the gift, its timing and value. For example, in the UK it is customary for small gifts to be given at Christmas;

(i) it is given openly, not secretly; and

(j) it complies with any applicable local law.]

7.2 Promotional gifts of low value such as branded stationery to or from existing customers, suppliers and business partners will usually be acceptable.

7.3 Reimbursing a third party's expenses, or accepting an offer to reimburse our expenses (for example, the costs of attending a business meeting) would not usually amount to bribery. However, a payment in excess of genuine and reasonable business expenses (such as the cost of an extended hotel stay) is not acceptable.

7.4 We appreciate that practice varies between countries and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift, hospitality or payment is reasonable and justifiable. The intention behind it should always be considered.

8. Donations

8.1 We do not make contributions to political parties.

8.2 We only make charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made without the prior approval of the **PATH Yorkshire Board of Trustees**.

9. Record-keeping

9.1 We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

9.2 You must declare and keep a written record of all hospitality or gifts given or received, which will be subject to managerial review.

9.3 You must submit all expenses claims relating to hospitality, gifts or payments to third parties in accordance with our expenses policy and record the reason for expenditure.

9.4 All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments.

10. Your responsibilities

10.1 You must ensure that you read, understand and comply with this policy.

10.2 The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

10.3 You must notify [your line manager OR the Compliance Manager [or the confidential helpline]] as soon as possible if you believe or suspect that a conflict with this policy has occurred, or may occur in the future. For example, if a client or potential client offers you something to gain a business advantage with us, or indicates to you that a gift or payment is required to secure their business. Further "red flags" that may indicate bribery or corruption are set out in clause 15.

11. How to raise a concern

11.1 You are encouraged to raise concerns about any issue or suspicion of bribery or corruption at the earliest possible stage.

11.2 If you are offered a bribe, or are asked to make one, or if you believe or suspect that any bribery, corruption or other breach of this policy has occurred or may occur, you must notify your line manager as soon as possible.

11.3 If you are unsure about whether a particular act constitutes bribery or corruption, raise it with your line manager.

12. Protection

12.1 Individuals who refuse to accept or offer a bribe, or who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

12.2 We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the Compliance Manager immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure, which is available [on the intranet OR from your line manager OR from the HR Department OR in this Staff Handbook].

13. Training and communication

13.1 Training on this policy forms part of the induction process for all individuals who work for us, and regular training will be provided as necessary.

13.2 Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

14. Breaches of this policy

14.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

14.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

15. Potential risk scenarios: "red flags"

15.1 The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only.

15.2 If you encounter any of these red flags while working for us, you must report them promptly to your manager.

(a) you become aware that a third party engages in, or has been accused of engaging in, improper business practices;

(b) you learn that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a "special relationship" with foreign government officials;

(c) a third party insists on receiving a commission or fee payment before committing to sign up to a contract with us, or carrying out a government function or process for us;

(d) a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

(e) a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

(f) a third party requests an unexpected additional fee or commission to "facilitate" a service;

(g) a third party demands lavish entertainment or gifts before commencing or continuing contractual negotiations or provision of services;

(h) a third party requests that a payment is made to "overlook" potential legal violations;

(i) a third party requests that you provide employment or some other advantage to a friend or relative;

(j) you receive an invoice from a third party that appears to be non-standard or customised;

(k) a third party insists on the use of side letters or refuses to put terms agreed in writing;

(l) you notice that we have been invoiced for a commission or fee payment that appears large given the service stated to have been provided;

(m) a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us;

(n) you are offered an unusually generous gift or offered lavish hospitality by a third party; or

Data protection policy

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company name: PATH Yorkshire.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): either of the following:

a) the person required to be appointed in specific circumstances under the UK GDPR; or

b) where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO or the Company data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: the Company privacy and UK GDPR-related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available from the HR Department.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on

the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available from your line manager **OR** from the DPO].

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Introduction

1.2 This Data Protection Policy sets out how PATH Yorkshire handle the Personal Data of our customers, prospective customers, suppliers, employees, workers, business contacts and other third parties.

1.3 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

1.4 This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the Company and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

1.5 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach, or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

1.6 This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the DPO.

2. Scope of Policy and when to seek advice on data protection compliance.

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we always take seriously. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

2.2 The CEO and all line managers, are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

2.3 The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Colvyn Inniss, and they can be reached at 01132624600 and *colvyn.inniss@pathyorkshire.co.uk*

2.4 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Company) (see paragraph 4.1);

(b) if you need to rely on Consent or need to capture Explicit Consent (see paragraph 5);

(c) if you need to draft Privacy Notices (see paragraph 6);

(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 10);

(e) if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 11.1);

(f) if there has been a Personal Data Breach (paragraph 12);

(g) if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 13);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 14);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 18) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 7);

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 19);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 20); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 21).

3. Personal data protection principles

3.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

4. Lawfulness, fairness and transparency

4.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful

purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

4.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices

4.4 You must identify and document the legal ground being relied on for each Processing activity [in accordance with the Company's guidelines on the Lawful Basis for Processing Personal Data, HR Department.

5. Consent

5.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

5.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

5.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines, so that the Company can demonstrate compliance with Consent requirements.

6. Transparency (notifying Data Subjects)

6.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

6.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

6.5 You must comply with the Company's guidelines on drafting Privacy Notices.

7. Purpose limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

8. Data minimisation

8.1 Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

9. Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. [You must comply with the Company's Data Retention Policy.]

10.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

10.5 You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

11. Security integrity and confidentiality

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users can access the Personal Data when they need it for authorised purposes.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data].

12. Reporting a Personal Data Breach

12.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

12.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

12.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (your line manager **OR** the DPO) You should preserve all evidence relating to the potential Personal Data Breach.

13. Transfer limitation

13.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

13.2 You must comply with the Company's guidelines on cross-border data transfers.

13.3 You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including:

(i) the performance of a contract between us and the Data Subject;

(ii) reasons of public interest;

(iii) to establish, exercise or defend legal claims;

(iv) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and

(v) in some limited cases, for our legitimate interest.

14. Data Subject's rights and requests

14.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority;

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and

14.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

14.3 You must immediately forward any Data Subject request you receive to [your line manager **OR** the HR Department **OR** the DPO] [and comply with the Company's Response procedures for data subject requests].

15. Accountability

15.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

15.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Company Personnel on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Record keeping

16.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

16.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents [in accordance with the Company's record-keeping guidelines].

16.3 These records should include, at a minimum:

(a) the name and contact details of the Controller and the DPO; and

(b) clear descriptions of:

(i) the Personal Data types;

(ii) the Data Subject types;

(iii) the Processing activities;

(iv) the Processing purposes;

(v) the third-party recipients of the Personal Data;

(vi) the Personal Data storage locations;

(vii) the Personal Data transfers;

(viii) the Personal Data's retention period; and

(ix) the security measures in place.

16.4 To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

17. Training and audit

17.1 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

17.2 You must undergo all mandatory data privacy-related training and ensure your team undergoes similar mandatory training in accordance with the Company's mandatory training guidelines.

17.3 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Privacy by Design and Data Protection Impact Assessment (DPIA)

18.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

18.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) The state of the art.

(b) The cost of implementation.

(c) The nature, scope, context and purposes of Processing.

(d) The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

18.3 The Controller must also conduct a DPIA in respect to high-risk Processing.

18.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

(b) Automated Processing including profiling and ADM.

(c) Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.

(d) Large-scale, systematic monitoring of a publicly accessible area.

18.5 A DPIA must include:

(a) A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.

(b) An assessment of the necessity and proportionality of the Processing in relation to its purpose.

(c) An assessment of the risk to individuals.

(d) The risk mitigation measures in place and demonstration of compliance.

18.6 You must comply with the Company's guidelines on DPIA and Privacy by Design.

19. Automated Processing (including profiling) and Automated Decision-Making

19.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

19.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This

right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

19.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

19.6 [Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Company's guidelines on profiling or ADM.] [Where you intend to use any generative AI tool, you must also comply with the Company's Generative AI Policy.]]

20. Direct marketing

20.1 We are subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example when sending marketing emails or making telephone sales calls).

20.2 For example, in a business to consumer context, a Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows an organisation to send marketing texts or emails without consent if it:

(a) Has obtained contact details in the course of a sale to that person.

(b) Is marketing similar products or services.

(c) Gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

20.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

20.4 A Data Subject's objection to direct marketing must always be promptly honoured. If a customer opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

20.5 You must comply with the Company's guidelines on direct marketing to customers and you should consult [the DPO] if you are unsure regarding how to comply with either the Company's guidelines or the law.

21. Sharing Personal Data

21.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

21.2 You must comply with the Company's guidelines on sharing data with third parties.

21.3 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

21.4 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

22. Changes to this Data Protection Policy

22.1 We keep this Data Protection Policy under regular review.

22.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

Health & Safety Policy

1. About this policy

1.1 We are committed to ensuring the health and safety of staff and anyone affected by our business activities, and to providing a safe and suitable environment for all those attending our premises.

1.2 The purpose of this policy is to set out our arrangements in relation to:

(a) assessment and control of health and safety risks arising from work activities;

(b) preventing accidents and work-related ill health;

(c) consultation with employees on matters affecting their health and safety;

(d) provision and maintenance of a safe workplace and equipment;

(e) information, instruction, training and supervision in safe working methods and procedures;

(f) emergency procedures in cases of fire or other major incident.

1.3 [This policy has been implemented by the PATH Yorkshire Board of Trustees.

1.4 This policy does not form part of any contract of employment or other contract to provide services and we may amend it at any time.

2. Who does this policy apply to?

2.1 This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns. It also applies to anyone visiting our premises or using our vehicles.

3. Who is responsible for this policy?

3.1 The PATH Yorkshire Board of Trustees has overall responsibility for the effective operation of this policy. The PATH Yorkshire Board of Trustees has delegated responsibility for overseeing its implementation to the Health and Safety Officer. Suggestions for changes to this policy should be reported to the Health and Safety Officer. The post of Health and Safety Officer is held by Sarah Brown, and can be contacted at *sarah.brown@pathyorkshire.co.uk* phone number 01132624600.

3.2 Any questions you may have about the day-to-day application of this policy should be referred to your line manager in the first instance.

3.3 This policy is reviewed annually by the Health and Safety Officer PATH Yorkshire Board of Trustees

4. Your responsibilities

4.1 All staff share responsibility for achieving safe working conditions. You must take care of your own health and safety and that of others, observe applicable safety rules and follow instructions for the safe use of equipment.

4.2 You should report any health and safety concerns immediately to line manager.

4.3 You must co-operate with managers on health and safety matters, including the investigation of any incident.

4.4 Failure to comply with this policy may be treated as misconduct and dealt with under our Disciplinary Procedure.

5. Information and consultation

5.1 We will inform and consult workplace safety directly with all staff regarding health and safety matters.

5.2 We will ensure any health and safety representatives receive the appropriate training to carry out their functions effectively.

5.3 The Health and Safety Officer is responsible for informing and consulting employees about health and safety matters.

6. Training

6.1 We will ensure that you are given adequate training and supervision to perform your work competently and safely.

6.2 Staff will be given a health and safety induction and provided with appropriate safety training

7. Equipment

7.1 You must use equipment in accordance with any instructions given to you. Any equipment fault or damage must immediately be reported to your line manager

7.2 No member of staff should attempt to repair equipment unless trained to do so.

7.3 The Health and Safety Officer is responsible for ensuring equipment safety and maintenance.

8. Accidents and first aid

8.1 Details of first aid facilities and the names of trained first aiders are displayed on the notice boards.

8.2 All accidents and injuries at work, however minor, should be reported to Health and Safety Officer and recorded in the Accident Book which is kept in Front Reception.

8.3 The Health and Safety Officer is responsible for investigating any injuries or work-related diseases, ensuring that accident records are kept, and for submitting reports to the relevant authorities if required under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (*SI 2013/1471*) (RIDDOR).

9. National health alerts

9.1 In the event of an epidemic or pandemic alert we will organise our business operations and provide advice on steps to be taken by staff, in accordance with official guidance, to reduce the risk of infection at work as far as possible. Any questions should be referred to [your line manager **OR** the HR Department] [or the Occupational Health Department].

9.2 It is important for the health and safety of all our staff that you comply with instructions issued in these circumstances.

10. Fire safety

10.1 All staff should familiarise themselves with the fire safety instructions, which are displayed on notice boards and near fire exits in the workplace.

10.2 If you hear a fire alarm, leave the building immediately by the nearest fire exit and go to [the fire assembly point shown on the fire safety notices Do not stop to collect belongings or use any lifts. Fire wardens will assist in the evacuation of the building and you must follow their instructions. Do not re-enter the building until told to do so.

10.3 If you discover a fire do not attempt to tackle it unless it is safe and you have been trained or feel competent to do so. You should operate the nearest fire alarm and, if you have sufficient time, call reception and report the location of the fire.

10.4 Nominated individuals will be trained in the correct use of fire extinguishers.

10.5 You should notify line manager if there is anything (for example, impaired mobility) that might impede your evacuation in the event of a fire. A personal evacuation plan will be drawn up and brought to the attention of the relevant fire wardens and colleagues working in your vicinity.

10.6 Fire drills will be held at least every 6 months and must be taken seriously.

10.7 The Health and Safety Officer is responsible for ensuring fire risk assessments are undertaken and implemented, and for ensuring regular checks of fire extinguishers, fire alarms, escape routes and emergency lighting.

11. Risk assessments and measures to control risk.

11.1 We carry out general workplace risk assessments periodically. The purpose is to assess the risks to health and safety of employees, visitors and other third parties as a result of our activities, and to identify any measures that need to be taken to control those risks.

11.2 Measures will be taken to avoid or reduce the need to lift or carry items which could cause injury (manual handling) and to provide training on manual handling as necessary.

11.3 The use of hazardous substances at work will be avoided wherever possible and less hazardous alternatives will be used where available. Training on the control of substances hazardous to health (COSHH) will be provided as necessary.

11.4 Personal protective equipment (PPE) is provided where there are risks that cannot be adequately controlled by other means.

11.5 The Health and Safety Officer is responsible for workplace risk assessments and any measures to control risks.

12. Computers and display screen equipment

12.1 If you use a computer screen or other display screen equipment (DSE) habitually as a significant part of your work:

(a) You should try to organise your activity so that you take frequent short breaks from looking at the screen.

(b) You are entitled to a workstation assessment.

(c) You are entitled to an eyesight test by an optician at our expense.

12.2 You should contact your line manager to request a workstation assessment or an eye test. Eye tests should be repeated at regular intervals as advised by the optician, usually every two years.

However, if you develop eye problems which may be caused by DSE work (such as headaches, eyestrain, or difficulty focusing) you can request a further eye test at any time.

12.3 We will not normally pay for glasses or contact lenses, unless your vision cannot be corrected by normal glasses or contact lenses and you need special glasses designed for the display screen distance. In such cases we will pay the cost of basic corrective appliances only.

12.4 Further information on the use of DSE can also be obtained from the HR Department.

Diversity, Equality and Inclusion Policy

1. Our commitments

1.1 We are committed to promoting equal opportunities in employment and creating a workplace culture in which diversity and inclusion is valued and everyone is treated with dignity and respect. As part of our zero-tolerance approach to discrimination in any form, you and any job applicants will receive equal treatment regardless of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation (**Protected Characteristics**). We are also committed to providing equitable treatment to all those we deal with as an organisation, including customers and suppliers.

1.2 We will take all reasonable steps to:

- Promote awareness and provide training to all staff and all managers on all aspects of equality and diversity in the workplace.
- Apply the principles of equity to all staff and all job applicants so that there is equality of opportunity. Our aim is that no individual is denied employment opportunities for reasons unrelated to ability.
- Establish programmes and processes that ensure a diversity of candidates at all career stages beginning with recruitment, including the development and promotion of talent through to the appointment of senior leadership.
- Implement all internal policies and procedures (on a fair and impartial basis).
- Create an inclusive working environment that is sensitive to the needs of staff of differing cultures, religions and beliefs. For example, in connection with festivals, religious observance and dress.
- Make reasonable adjustments to enable employees with disabilities to function effectively and to their full potential.
- Ensure that all work environments are free from all forms of discrimination, harassment, intimidation or bullying.
- Monitor how this policy is working in practice.

2. About this policy

2.1 The purpose of this policy is to set out our approach to diversity, equity and inclusion. Our aim is to encourage and support diversity, equity and inclusion and actively promote a culture that values difference and eliminates discrimination in our workplace. It applies to all aspects of employment with us, including recruitment, pay, benefits and conditions, flexible working and leave, training, appraisals, promotion, conduct at work, disciplinary and grievance procedures, and termination of employment.

2.2 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

3. Who does this policy apply to?

3.1 This policy applies to all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

4. Who is responsible for this policy?

4.1 All managers must set an appropriate standard of behaviour, lead by example and ensure that those they manage adhere to the policy and promote our aims and objectives with regard to diversity, equity and inclusion.

4.2 This policy is reviewed annually by PATH Yorkshire Board of Trustees

5. Diversity and inclusion training

5.1 Managers will be given appropriate training on recognising and avoiding discrimination, harassment, victimisation[, unconscious bias] and promoting equality of opportunity and diversity in the areas of recruitment, development and promotion. The CEO has overall responsibility for equality training for staff and managers, as appropriate.

5.2 We will provide you with regular training to ensure that everyone is aware of and understands the contents of this policy. Following the training, you will be required to confirm that you have read, understand and will comply with this policy.

6. Discrimination

6.1 You must not unlawfully discriminate against or harass other people, including current and former staff, job applicants, clients, customers, suppliers and visitors. This applies in the workplace, outside the workplace (when dealing with customers, suppliers or other work-related

contacts or when wearing a work uniform), and on work-related trips or events including social events.

6.2 The following forms of discrimination are prohibited under this policy and are unlawful:

(a) **Direct discrimination:** treating someone less favourably because of a Protected Characteristic. For example, rejecting a job applicant because of their religious views or because they might be gay. Direct discrimination can include associative discrimination, where a person is treated less favourably because of their association with an individual with a Protected Characteristic, and perception discrimination, where a person is treated less favourably because of the mistaken belief that they possess a Protected Characteristic.

(b) **Indirect discrimination:** a provision, criterion or practice that applies to everyone but adversely affects people with a particular Protected Characteristic more than others, and is not justified. For example, requiring a job to be done full-time rather than part-time would adversely affect women because they generally have greater childcare commitments than men. Such a requirement would be discriminatory unless it can be justified.

(c) **Harassment:** this includes sexual harassment and other unwanted conduct related to a Protected Characteristic, which has the purpose or effect of violating someone's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. [Harassment is dealt with further in our Anti-harassment and Bullying Policy.]

(d) **Victimisation:** retaliation against someone who has complained or has supported someone else's complaint about discrimination or harassment. This includes where someone mistakenly believes that the person victimised has done so.

(e) **Disability discrimination:** this includes direct and indirect discrimination, any unjustified less favourable treatment because of the effects of a disability, and failure to make reasonable adjustments to alleviate disadvantages caused by a disability.

7. Recruitment and selection

7.1 Recruitment, promotion, and other selection exercises such as redundancy selection will be conducted on the basis of merit, against objective criteria that avoid discrimination. When recruiting or promoting, we will aim to take steps to improve the diversity of our workforce and provide equality of opportunity. Shortlisting [and interviewing] should be done by more than one person and with the involvement of the HR Department, where possible. Our recruitment procedures will be reviewed regularly to ensure that individuals are objectively assessed on the basis of their relevant merits and abilities.

7.2 Vacancies should generally be advertised to a diverse section of the labour market by [using a variety of social media channels as well as] using recruitment agencies which provide a diverse range of suitable candidates. Advertisements should avoid stereotyping or using wording that may discourage particular groups from applying. They should include a short policy statement on equal opportunities and the employer's commitment to diversity, equity and inclusion in the workplace and state that a copy of this policy will be made available on request.

7.3 Job applicants should not be asked questions which might suggest an intention to discriminate on grounds of a Protected Characteristic. For example, applicants should not be asked whether they are pregnant or planning to have children.

7.4 Job applicants should not be asked about health or disability before a job offer is made. There are limited exceptions which should only be used with the approval of the HR Department. For example:

(a) Questions necessary to establish if an applicant can perform an intrinsic part of the job (subject to any reasonable adjustments).

(b) Questions to establish if an applicant is fit to attend an assessment or any reasonable adjustments that may be needed at interview or assessment.

(c) Positive action to recruit disabled persons.

(d) Equal opportunities monitoring (which will not form part of the selection or decision-making process).

Where necessary, job offers can be made conditional on a satisfactory medical check.

7.5 We are required by law to ensure that all employees are entitled to work in the UK. Assumptions about immigration status should not be made based on appearance or apparent nationality. All prospective employees, regardless of nationality, must be able to produce original documents (such as a passport) before employment starts, to satisfy current immigration legislation. The list of acceptable documents is available from the HR Department or UK Visas and Immigration.

7.6 To ensure that this policy is operating effectively, and to identify groups that may be underrepresented or disadvantaged in our organisation, we monitor applicants' ethnic group, nationality, gender, gender identity, disability, sexual orientation, religion and age as part of the recruitment procedure. Provision of this information is voluntary and it will not adversely affect an individual's chances of recruitment or any other decision related to their employment. The information is removed from applications before shortlisting, and kept in an anonymised format solely for the purposes stated in this policy and in accordance with data protection legislation. Analysing this data helps us take appropriate steps to avoid discrimination and improve equality, diversity and inclusion.

8. Training, promotion and conditions of service

8.1 Training needs will be identified through regular appraisals which will be based entirely on an objective assessment of performance and will not be influenced by any Protected Characteristics that you may have. You will be given appropriate access to training to enable you to progress within the organisation and all promotion decisions will be made on the basis of merit.

9. Monitoring

9.1 We will monitor the effectiveness of our policies and procedures in meeting our diversity, equity and inclusion objectives and to identify areas in which further resources or support are required to achieve equality of experience.

9.2 We will also monitor the treatment and outcomes of any complaints of discrimination, harassment or victimisation we receive to ensure that they are properly investigated and resolved, those who report or act as witnesses are not victimised, repeat offenders are dealt with appropriately, cultural clashes are identified and resolved and workforce training is targeted where needed.

9.3 We will regularly share with you the progress and achievements we have made towards our diversity, equity and inclusion objectives.

10. Termination of employment

10.1 We will ensure that redundancy criteria and procedures are fair and objective and are not directly or indirectly discriminatory.

10.2 We will also ensure that disciplinary procedures and penalties are applied without discrimination, whether they result in disciplinary warnings, dismissal or other disciplinary action.

11. Disabilities

11.1 If you are disabled or become disabled, we encourage you to tell us about your condition so that we can support you as appropriate.

11.2 If you experience difficulties at work because of your disability, you may wish to contact [your line manager **OR** the HR Department] to discuss any reasonable adjustments that would help overcome or minimise the difficulty. [Your line manager **OR** The HR Department] may wish to consult with you and your medical adviser about possible adjustments. We will consider the matter carefully and try to accommodate your needs within reason. If we consider a particular

adjustment would not be reasonable, we will explain our reasons and try to find an alternative solution where possible.

11.3 We will monitor the physical features of our premises to consider whether they might place anyone with a disability at a substantial disadvantage. Where necessary, we will take reasonable steps to improve access.

12. Part-time and fixed-term work

12.1 Part-time and fixed-term staff should be treated the same as comparable full-time or permanent staff and enjoy no less favourable terms and conditions (on a pro-rata basis where appropriate), unless different treatment is justified.

13. Breaches of this policy

13.1 We take a strict approach to breaches of this policy, which will be dealt with in accordance with our Disciplinary Procedure. Serious cases of deliberate discrimination and victimisation may amount to gross misconduct resulting in dismissal.

13.2 If you believe that you have suffered harassment, bullying or discrimination, or witnessed it happening to someone else in the workplace, you can raise the matter using the procedure set out in this policy. Complaints will be treated in confidence and investigated as appropriate.

13.3 There must be no victimisation or retaliation against staff who complain about or report discrimination. If you believe you have been victimised for making a complaint or report of discrimination, or have witnessed it happening to someone else in the workplace, you should raise this through the procedure set out in this policy.

13.4 We encourage the reporting of all types of potential discrimination, as this assists us in ensuring that diversity, equity and inclusion principles are adhered to in the workplace. However, making a false allegation in bad faith, or that you know to be untrue, will be treated as misconduct and dealt with under our Disciplinary Procedure.

14. Related policies

14.1 This policy is supported by the following other policies and procedures:

(a) Anti-harassment and Bullying Policy.

(b) Grievance Procedure.

(c) Disciplinary Procedure.

(d) Gender Identity Policy.

(e) Flexible Working Procedure.

(f) Maternity, Paternity, Adoption and Shared Parental Leave Policies.

(g) Parental Leave Policy.

(h) Time Off for Dependants Policy.

(i) Dress Code.

(j) Homeworking Policy.

(k) Hybrid Working Policy.

(l) Career Break Policy.

Whistleblowing Policy

1. About this policy

1.1 We are committed to conducting our business with honesty and integrity, and we expect all staff to maintain high standards [in accordance with our Code of Conduct]. However, all organisations face the risk of things going wrong from time to time, or of unknowingly harbouring illegal or unethical conduct. A culture of openness and accountability is essential to prevent such situations occurring and to address them when they do occur.

1.2 The purpose of this policy is:

(a) To encourage staff to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate, and that their confidentiality will be respected.

(b) To provide staff with guidance as to how to raise those concerns.

(c) To reassure staff that they should be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken.

1.3 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time

2. Who does this policy apply to?

2.1 This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns.

3. Who is responsible for this policy?

3.1 The PATH Yorkshire Board of Trustees [has overall responsibility for the effective operation of this policy, and for reviewing the effectiveness of actions taken in response to concerns raised under this policy.

3.2 The CEO has day-to-day operational responsibility for this policy and you should refer any questions about this policy to them in the first instance. The CEO must ensure that regular and appropriate training is provided to all managers and other staff who may deal with concerns or investigations under this policy.

3.3 This policy is reviewed at least annually by the CEO and the PATH Yorkshire Board of Trustees

3.4 All staff are responsible for the success of this policy and should ensure that they use it to disclose any suspected danger or wrongdoing. Staff are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the CEO who will involve the PATH Yorkshire Board of Trustees [where appropriate.

4. What is whistleblowing?

4.1 **Whistleblowing** is the disclosure of information which relates to suspected wrongdoing or dangers at work. This may include:

(a) criminal activity;

(b) failure to comply with any legal [or professional] obligation [or regulatory requirements];

(c) miscarriages of justice;

(d) danger to health and safety;

(e) damage to the environment;

(f) bribery under our Anti-corruption and Bribery Policy;

(g) financial fraud or mismanagement;

(h) breach of our internal policies and procedures including our Code of Conduct];

(i) conduct likely to damage our reputation or financial wellbeing;

(j) unauthorised disclosure of confidential information;

(k) negligence;

(l) the deliberate concealment of any of the above matters.

4.2 A **whistleblower** is a person who raises a genuine concern relating to any of the above. If you have any genuine concerns related to suspected wrongdoing or danger affecting any of our activities (a **whistleblowing concern**) you should report it under this policy.

4.3 This policy should not be used for complaints relating to your own personal circumstances, such as the way you have been treated at work. In those cases you should use the Grievance Procedure [or Anti-harassment and Bullying Policy as appropriate].

4.4 If a complaint relates to your own personal circumstances but you also have wider concerns regarding one of the areas set out at paragraph 4.1 above (for example, a breach of our internal policies), you should discuss with the CEO which route is the most appropriate.

4.5 If you are uncertain whether something is within the scope of this policy you should seek advice from CEO whose contact details are at the end of this policy.

5. Raising a whistleblowing concern

5.1 We hope that in many cases you will be able to raise any concerns with your line manager. You may tell them in person or put the matter in writing if you prefer. They may be able to agree a way of resolving your concern quickly and effectively. In some cases they may refer the matter to the CEO.

5.2 However, where the matter is more serious, or you feel that your line manager has not addressed your concern, or you prefer not to raise it with them for any reason, you should contact one of the following:

(a) The CEO **or a member of the Board of Trustees** (Contact details are set out at the end of this policy).

5.3 We will arrange a meeting with you as soon as possible to discuss your concern. You may bring a colleague or union representative to any meetings under this policy. Your companion must respect the confidentiality of your disclosure and any subsequent investigation.

5.4 We will take down a written summary of your concern and provide you with a copy after the meeting. We will also aim to give you an indication of how we propose to deal with the matter.

6. Confidentiality

6.1 We hope that staff will feel able to voice whistleblowing concerns openly under this policy. However, if you want to raise your concern confidentially, we will make every effort to keep your identity secret. If it is necessary for anyone investigating your concern to know your identity, we will discuss this with you.

6.2 We do not encourage staff to make disclosures anonymously, although we will make every effort to investigate anonymous disclosures. You should be aware that proper investigation may be more difficult or impossible if we cannot obtain further information from you. It is also more difficult to establish whether any allegations are credible. Whistleblowers who are concerned about possible reprisals if their identity is revealed should come forward to the Whistleblowing Officer **OR** The Board of Trustees or one of the other contact points listed in paragraph 5 and appropriate measures can then be taken to preserve confidentiality. If you are in any doubt, you can seek advice from the Citizens Advice or ACAS, or Protect, the independent whistleblowing charity, who offer a confidential helpline. Their contact details are at the end of this policy.

7. Investigation and outcome

7.1 Once you have raised a concern, we will carry out an initial assessment to determine the scope of any investigation. We will inform you of the outcome of our assessment. You may be required to attend additional meetings in order to provide further information.

7.2 In some cases we may appoint an investigator or team of investigators including staff with relevant experience of investigations or specialist knowledge of the subject matter. The investigator (or investigators) may make recommendations for change to enable us to minimise the risk of future wrongdoing.

7.3 We will aim to keep you informed of the progress of the investigation and its likely timescale. However, sometimes the need for confidentiality may prevent us giving you specific details of the investigation, an outcome or any disciplinary action taken as a result. You should treat any information about the investigation as confidential.

7.4 If we conclude that a whistleblower has made false allegations maliciously, the whistleblower will be subject to disciplinary action.

8. If you are not satisfied

8.1 While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and in an appropriate way. By using this policy, you can help us to achieve this.

8.2 If you are not happy with the way in which your concern has been handled, you can raise it with one of the other key contacts in paragraph 5. Alternatively, you may contact the [Chair of the Board **of Trustees** or our external auditors. Contact details are set out at the end of this policy.

9. External disclosures

9.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.

9.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. It will very rarely if ever be appropriate to alert the media. We strongly encourage you to seek advice before reporting a concern to anyone external. The independent whistleblowing charity, Protect, operates a confidential helpline. They also have a list of prescribed regulators for reporting certain types of concern. Their contact details are at the end of this policy.

9.3 Whistleblowing concerns usually relate to the conduct of our staff, but they may sometimes relate to the actions of a third party, such as a [Learner, supplier, or service provider. In some circumstances the law will protect you if you raise the matter with the third party directly. However, we encourage you to report such concerns internally first, in line with this policy. You should contact your line manager or [one of] the other individuals set out in paragraph 5 for guidance.

10. Protection and support for whistleblowers

10.1 It is understandable that whistleblowers are sometimes worried about possible repercussions. We aim to encourage openness and will support staff who raise genuine concerns under this policy, even if they turn out to be mistaken.

10.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the CEO or the HR Department] immediately. If the matter is not remedied, you should raise it formally using our Grievance Procedure.

10.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct, you may be subject to disciplinary action. [In some cases, the whistleblower could have a right to sue you personally for compensation in an employment tribunal.]

10.4 [A confidential support and counselling hotline is available to whistleblowers who raise concerns under this policy. Their contact details are set out at the end of this policy.]

11. Contacts

[Whistleblowing Officer OR [POSITION]]	[NAME] [TELEPHONE] [EMAIL]
CEO	Vernon Richardson O1132624600 Vernon.richardson@pathyorkshire.co.uk

[Chair of the Board OR Chair of the [COMMITTEE] OR [POSITION] OR Chair of the Audit Committee]	Melvin Wyatt O1132624600
[EMPLOYER'S] external auditors	[COMPANY NAME] [TELEPHONE] [EMAIL]
Protect (Independent whistleblowing charity)	Helpline: 020 3117 2520 Website: *https://protect-advice.org.uk*

Safeguarding Policy

1. Purpose

Our charitable activities include working with vulnerable people. The purpose of this policy is to protect them and provide stakeholders and the public with the overarching principles that guide our approach in doing so.

2. Lead Trustee

A lead trustee will be appointed to provide oversight of safeguarding and to lead on any incident investigation and reporting.

Lead Trustee	Melvin Wyatt

3. Applicability

3.1 This policy applies to anyone working on our behalf, including our trustees and other volunteers.

3.2 Partner organisations will be required to have their own safeguarding procedures that must, as a minimum, meet the standards outlined below, and include any additional legal or regulatory requirements specific to their work. These include, but are not limited to other UK regulators, if applicable.

3.3 Safeguarding should be appropriately reflected in other relevant policies and procedures.

4. Principles

We believe that:

- Nobody who is involved in our work should ever experience abuse, harm, neglect or exploitation.
- We all have a responsibility to promote the welfare of all of our beneficiaries, staff and volunteers, to keep them safe and to work in a way that protects them.
- We all have a collective responsibility for creating a culture in which our people not only feel safe, but also able to speak up, if they have any concerns.

5. Types of Abuse

Abuse can take many forms, such as physical, psychological or emotional, financial, sexual or institutional abuse, including neglect and exploitation. Signs that may indicate the different types of abuse are at Appendix 1.

6. Reporting Concerns

If a crime is in progress, or an individual in immediate danger, call the police, as you would in any other circumstances.
If you are a beneficiary, or member of the public, make your concerns known to a member of our team, who will alert a senior member of the charity.

For members of the charity, make your concerns known to your supervisor. If you feel unable to do so, speak to a trustee.

The trustees are mindful of their reporting obligations to the Charity Commission in respect of Serious Incident Reporting and, if applicable, other regulator. They are aware of the Government guidance on handling safeguarding allegations.

7. Responsibilities

7.1 Trustees

This safeguarding policy will be reviewed and approved by the Board annually.
Trustees are aware of and will comply with the Charity Commission guidance on safeguarding and protecting people and also the 10 actions trustee boards need to take to ensure good safeguarding governance.

A lead trustee/committee with be given responsibility for the oversight of all aspects of safety, including whistleblowing and H&SW. This will include:

- Creating a culture of respect, in which everyone feel safe and able to speak up.
- An annual review of safety, with recommendations to the Board.
- Receiving regular reports, to ensure this and related policies are being applied consistently.
- Providing oversight of any lapses in safeguarding.
- And ensuring that any issues are properly investigated and dealt with quickly, fairly and sensitively, and any reporting to the Police/statutory authorities is carried out.
- Leading the organisation in way that makes everyone feels safe and able to speak up.

- Ensuring safeguarding risk assessments are carried out and appropriate action taken to minimise these risks, as part of our risk management processes.
- Ensuring that all relevant checks are carried out in recruiting staff and volunteers.
- Planning programmes/activities to take into account potential safeguarding risks, to ensure these are adequately mitigated.
- Ensuring that all appointments that require DBS clearance and safeguarding training are identified, including the level of DBS and any training required.
- Ensuring that a central register is maintained and subject to regular monitoring to ensure that DBS clearances and training are kept up-to-date.
- Ensuring that safeguarding requirements (e.g. DBS) and responsibilities are reflected in job descriptions, appraisal objectives and personal development plans, as appropriate.
- Listening and engaging, beneficiaries, staff, volunteers and others and involving them as appropriate.
- Responding to any concerns sensitively and acting quickly to address these.
- Ensuring that personal data is stored and managed in a safe way that is compliant with data protection regulations, including valid consent to use any imagery or video.
- Making staff, volunteers and others aware of:
    - Our safeguarding procedures and their specific safeguarding responsibilities on induction, with regular updates/reminders, as necessary.
    - The signs of potential abuse and how to report these.

7.2 Everyone

To be aware of our procedures, undertake any necessary training, be aware of the risks and signs of potential abuse and, if you have concerns, to report these immediately (see above).

8. Fundraising

We will ensure that:

- We comply with the Code of Fundraising Practice, including fundraising that involves children.
- Staff and volunteers are made aware of the Institute of Fundraising guidance on keeping fundraising safe and the NCVO Guidance on vulnerable people and fundraising.
- Our fundraising material is accessible, clear and ethical, including not placing any undue pressure on individuals to donate.
- We do not either solicit nor accept donations from anyone whom we know or think may not be competent to make their own decisions.
- We are sensitive to any particular need that a donor may have.

9. Online Safety

We will identify and manage online risks by ensuring:

- Volunteers, staff and trustees understand how to keep themselves safe online. We may use high privacy settings and password access to meetings to support this.
- The online services we provide are suitable for our users. For example, use age restrictions and offer password protection to help keep people safe.
- The services we use and/or provide are safe and in line with our code of conduct.
- We protect people's personal data and follow data protection legislation.
- We have permission to display any images on our website or social media accounts, including consent from an individual, parent, etc.
- We clearly explain how users can report online concerns. Concerns may be reported using this policy, or direct to a social media provider using their reporting process. If you are unsure, you can contact one of these organisations, who will help you.
- We have adopted and comply with the Charity AI Ethics & Governance Framework.

10. Working with Other Organisations

In working with other organisations, including any grant making, we will comply with Charity Commission guidance by carrying out relevant due diligence and having a written agreement that sets out:

- Our relationship.
- The role of each organisation.
- Monitoring and reporting arrangements.

Customer-Learner Complaints Procedure

At PATH Yorkshire, we value the feedback and concerns of our learners. We strive to provide a positive and supportive learning environment. However, we understand that there may be instances when learners may have complaints or issues that need to be addressed.

This Learner Complaints Procedure outlines the steps to follow when raising a complaint and ensures that all concerns are handled promptly, fairly, and confidentially.

Informal Resolution

We encourage learners to resolve complaints informally whenever possible. This step allows for open communication and swift resolution of concerns. Learners should follow these steps:

a. Discuss the Concern: The learner should raise the complaint with the person directly involved in the issue, such as the tutor, trainer, or relevant staff member. This conversation should take place in a calm and respectful manner, explaining the concern and seeking a resolution.

b. Escalate if Necessary: If the complaint remains unresolved or the learner feels uncomfortable discussing the matter with the person involved, they should escalate the concern to the next level of authority. This may involve contacting the department manager, course coordinator, or designated complaints officer.

Formal Complaint Process

If the complaint is not resolved through informal means or if the nature of the complaint requires immediate escalation, learners can follow the formal complaint process outlined below:

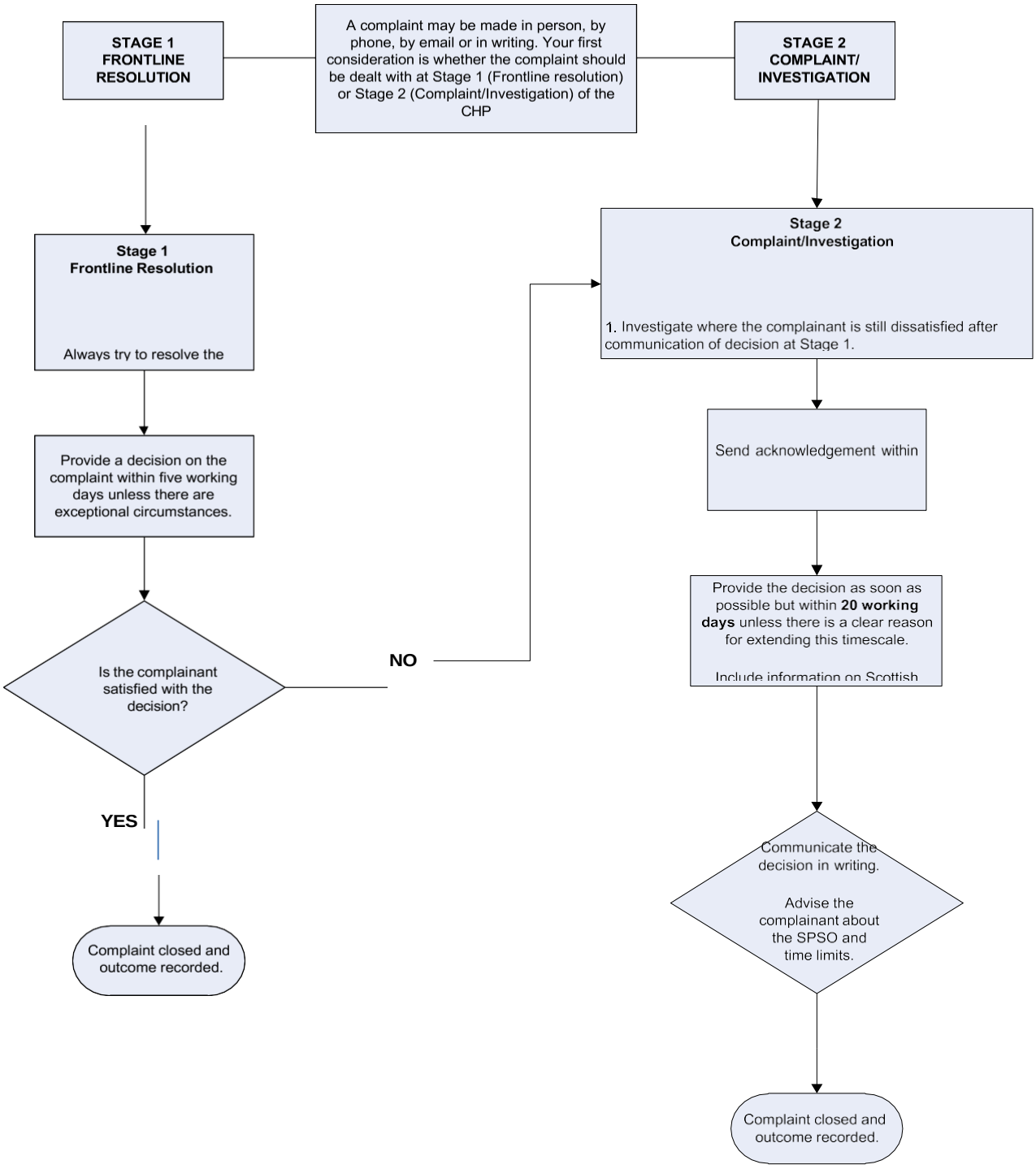
a. Submitting a Written Complaint: The learner should submit a written complaint, detailing the nature of the complaint, including any relevant dates, times, and individuals involved. This written complaint should be addressed to the complaints officer or relevant designated contact person.

b. Complaint Acknowledgment: Upon receiving the written complaint, the complaints officer will acknowledge receipt within a specified timeframe within three working days. The acknowledgment should include information on the expected timeframe for resolution.

c. Investigation and Resolution: The complaints officer will conduct a thorough investigation into the complaint, which may involve gathering additional information, interviewing relevant parties, or reviewing relevant documents. The complaints officer will aim to resolve the complaint within a reasonable timeframe, keeping the learner informed of the progress.

d. Complaint Outcome and Response: Once the investigation is complete, the complaints officer will communicate the outcome to the learner in writing. The response will include details of the findings, any actions taken to address the complaint, and any further steps to be taken if necessary.

PATH Yorkshire Customer-Learner COMPLAINTS HANDLING PROCEDURE



Secure Disposal of IT Equipment and Information Policy

1. Introduction

The PATH Yorkshire holds and processes a large amount of information and is required to protect that information in line with relevant legislation and in conformity with PATH Yorkshire regulations and policies such as the Information Security Policy, the Data Protection Policy and the Records Management Policy. This policy sets out the requirements for staff on the secure disposal of the PATH Yorkshire's IT equipment and information.

2. Definitions

2.1 Secure Disposal

Secure disposal means the process and outcome by which information including information held on IT equipment is irretrievably destroyed in a manner which maintains the security of the equipment and information during the process and up to the point of irretrievable destruction

2.2 IT Equipment

IT equipment means all equipment purchased by or provided by the PATH Yorkshire to store or process information including but not necessarily limited to desktop computers, servers, printers, copiers, laptops, tablet computers, electronic notebooks, mobile telephones, digital recorders, cameras, USB sticks, DVDs, CDs and other portable devices and removable media.

2.3 Information

2.3.1 Information means all information and data held or recorded electronically on IT equipment or manually held or recorded on paper.

2.3.2 For the purpose of this policy, the information held by the PATH Yorkshire can be divided into two categories: non-sensitive and sensitive information. Sensitive information comprises: all personal information and all confidential information, the loss of which would, or would be likely to, cause damage or distress to individuals or to the PATH Yorkshire.

The default category is that all information is deemed to be sensitive unless specifically identified as otherwise.

3. Responsibilities

3.1 It is the responsibility of all PATH Yorkshire staff to ensure that the information held by the PATH Yorkshire is disposed of appropriately and that all sensitive information is disposed of securely.

3.2 Responsibility for this policy resides with the PATH Yorkshire's Executive Board. Implementation of this policy is managed through the PATH Yorkshire's Information Security Working Group which reports to the Chief Information Officer.

4. Statement of Policy

4.1 This policy on disposal covers all data or information held by the PATH Yorkshire whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy.

4.2 It is the PATH Yorkshire's policy to ensure that all information held by the PATH Yorkshire is disposed of appropriately, in conformity with the PATH Yorkshire's legal obligations and in accordance with the PATH Yorkshire's regulations[link] and Records Management policy[link].

4.3 In particular it is the PATH Yorkshire's policy to ensure that all sensitive information which requires disposal is disposed of securely.

4.4 Where information is held on IT equipment, it is the policy of the PATH Yorkshire that such equipment will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely.

The PATH Yorkshire supports policies which promote sustainability and take account of environmental impact. The PATH Yorkshire will therefore support recycling or sustainable redeployment in the disposal of IT equipment as long as information held on the equipment is irretrievably and securely destroyed prior to the disposal of the equipment.

4.5 WEEE: IT equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006. [Link www.brookes.ac.uk/Documents/About/Sustainability/en103w2/]

4.6 Copyright: software must be disposed of in line with copyright legislation and software licensing provisions.

5. Policy Principles

5.1 Hard copy

5.1.1 Information and data held in paper or hard copy which contain sensitive information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, pulping or incineration.

5.1.2 The process leading to and the process of shredding, pulping or incinerating such information shall be carried out securely.

5.1.3 Where the shredding or incineration are carried out on behalf of the PATH Yorkshire by a third party, there shall be a contract with that third party which appropriately evidences:

a) that party's obligations to keep that data confidential and;

b) that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

5.1.4 Where hard copy information is stored externally by a third-party data storage contractor, the contract shall ensure secure disposal of the data at a time which conforms with the PATH Yorkshire's Retention Schedule[link].

5.2 IT Equipment

5.2.1 Since the policy default is that all IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction, or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

5.2.2 Where an overwrite procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed.

5.2.3 For the avoidance of doubt, removable digital media including but not limited to CDs, DVDs, USB drives, where the default is that they contain sensitive data, shall, if not successfully overwritten, be physically destroyed to the extent that all data contained in the media are irretrievable.

5.2.4 All IT equipment awaiting disposal must be stored and handled securely.

5.2.5 Where the overwriting procedure and/or physical destruction of IT equipment are

carried out on behalf of the PATH Yorkshire by a third party, there shall be a contract with that third party which appropriately evidences: that party's obligations to keep that data confidential and; that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

5.2.6 In any case where IT equipment is to be passed on by the PATH Yorkshire for re-use, those staff involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed.

5.2.7 Photocopiers and printers used or owned by the PATH Yorkshire may have a data storage capacity. Where such IT equipment contains information or data, the disposal of such equipment must have due regard to this policy.

5.3 Online Data

5.3.1 The PATH Yorkshire has a contract with Google for the use of its Google Apps for Education. This enables PATH Yorkshire staff to take advantage of the features provided for data storage of emails and documents. PATH Yorkshire does not sanction the use of external online (cloud) services for PATH Yorkshire data where there is no contract in place.

5.3.2 Data held in the PATH Yorkshire's Google applications or other authorised online storage applications should be destroyed to the extent possible by using the delete facilities provided.

5.4 Record of Destruction

5.4.1 Any third party contracted to dispose of sensitive hard copy information shall certify the irretrievable destruction of the information.

5.4.2 PATH Yorkshire staff who have responsibility for the information which is disposed of shall ensure that the disposal conforms with the PATH Yorkshire's Records Management policy[link] and Retention Schedule and that, where necessary, a record is kept documenting the disposal.

5.4.3 Where the disposal involves the disposal of IT equipment, the PATH Yorkshire shall keep a record of the asset number of the equipment which has been disposed of along with a record of the process by which the information stored on the equipment has been irretrievably destroyed.

6. Reporting

All staff, learners and other users of information should report immediately to the PATH Yorkshire managers any observed or suspected incidents where sensitive information has or may have been insecurely disposed of.

7. Guidelines

7.1 Hard Copy

7.1.1 Staff holding PATH Yorkshire data in hard copy should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. Further information can be obtained from the PATH Yorkshire Records Manager

7.1.2 It is good practice to shred, pulp or incinerate all PATH Yorkshire data which requires destruction. Where hard copy waste is sensitive data (as defined in 2.3.2) it should always be securely and irretrievably destroyed by shredding, pulping or incineration. To ensure the secure and irretrievable destruction of hard copy, staff are required to use the service provided by the PATH Yorkshire's selected contractor for the destruction of confidential waste.

7.1.3 Confidential waste bags for information requiring secure destruction can be provided by PATH Yorkshire which will collect the bags when they are ready for disposal. Bags which contain confidential waste should be sealed and kept secure until collected designated secure information disposal contractor.

7.1.4 Confidential waste bags awaiting collection or further processing should not be left in public areas or areas where they can be accessed by unauthorised staff/personnel.

7.1.5 Where sensitive data are stored under contract externally, staff responsible for the contract should ensure the contract includes secure, certificated destruction of the data in accordance with the appropriate retention period. External storage and destruction of PATH Yorkshire data should not be arranged without reference to the PATH Yorkshire Records Manager.

7.1.6 Where staff consider a document is of sufficient historic importance to be retained by the PATH Yorkshire, they should consult the PATH Yorkshire Archivist.

7.2 IT Equipment

7.2.1 Staff holding PATH Yorkshire data on IT equipment should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. In determining whether and when the data should be disposed of, staff should consult the PATH Yorkshire's Retention Schedule

7.2.2 Where a decision has been made that data held on IT devices or media should not be retained, the files containing the data should be deleted from those devices. Deletion involves putting the information "beyond use" by the user of the device or media. Data held in a recycling "bin" on the device or data which can easily be recovered by the user are not regarded as being "beyond use" and may still be subject to discovery and disclosure under information law (Freedom of Information, Subject Access Request) or litigation.

7.2.3 Staff shall never dispose of PATH Yorkshire IT equipment (devices or media) without taking steps to ensure the irretrievable deletion of data held on the equipment.

7.2.4 Electronic or digital data which have been put "beyond use" by users may still be reconstituted by IT specialists or by forensic computer analysts. This means that when IT equipment (devices or media) are disposed of, the data should be:

7.2.4.1 irretrievably destroyed by being overwritten in accordance with the appropriate industry standard, or

7.2.4.2 the hard disc containing the data within the equipment or the media containing the data (e.g. CD, USB stick) should be physically destroyed.

PATH Yorkshire has some shredding machines available which can destroy CDs and DVDs as well as shred hard copy.

7.2.5 Staff requiring the disposal of IT equipment which holds or may hold PATH Yorkshire data should contact the information officer. to arrange for the disposal.

7.2.6 Staff should also be mindful that PATH Yorkshire mobile telephones contain data which will need to be extracted or deleted from the device before the device is disposed of. The telephone should be returned to the Service Desk should be contacted to initiate the secure return and disposal of the device.

7.2.7 Where PATH Yorkshire staff are leasing equipment (such as multi-functional copiers), staff responsible for the contracts should ensure that the leasing contract certifies the secure disposal of any PATH Yorkshire data held on the devices during the period of lease.

7.2.8 When disposing of IT equipment, staff must be mindful of the WEEE regulations.

7.3 Online data

7.3.1 Staff using the delete facility provided by Google in the PATH Yorkshire's online Google applications should be aware that the deleted material will be held for 30 days in their online "bin". Such data will not be regarded as "beyond use" until it has been further deleted from the "bin".

7.3.2 Online data held in Google accounts provided to staff by the PATH Yorkshire for the purpose of their employment are not automatically deleted when staff leave the PATH Yorkshire. These accounts are deactivated and access to the data retained for any necessary business purpose. Prior to leaving the PATH Yorkshire, staff should, wherever possible, ensure the appropriate management and handover of the PATH Yorkshire data in their accounts, deleting from their accounts data which are no longer required by the PATH Yorkshire.

Appendix 1 – Signs of Abuse

Physical Abuse

- bruises, black eyes, welts, lacerations, and rope marks.
- broken bones.
- open wounds, cuts, punctures, untreated injuries in various stages of healing.
- broken eyeglasses/frames, or any physical signs of being punished or restrained.
- laboratory findings of either an overdose or under dose medications.
- individual's report being hit, slapped, kicked, or mistreated.
- vulnerable adult's sudden change in behaviour.
- the caregiver's refusal to allow visitors to see a vulnerable adult alone.

Sexual Abuse

- bruises around the breasts or genital area.
- unexplained venereal disease or genital infections.
- unexplained vaginal or anal bleeding.
- torn, stained, or bloody underclothing.
- an individual's report of being sexually assaulted or raped.

Mental Mistreatment/Emotional Abuse

- being emotionally upset or agitated.
- being extremely withdrawn and non-communicative or non-responsive.
- nervousness around certain people.
- an individual's report of being verbally or mentally mistreated.

Neglect

- dehydration, malnutrition, untreated bed sores and poor personal hygiene.
- unattended or untreated health problems.
- hazardous or unsafe living condition (e.g., improper wiring, no heat or running water).

- unsanitary and unclean living conditions (e.g., dirt, fleas, lice on person, soiled bedding, faecal/urine smell, inadequate clothing).
- an individual's report of being mistreated.

Self-Neglect

- dehydration, malnutrition, untreated or improperly attended medical conditions, and poor personal hygiene.
- hazardous or unsafe living conditions.
- unsanitary or unclean living quarters (e.g., animal/insect infestation, no functioning toilet, faecal or urine smell).
- inappropriate and/or inadequate clothing, lack of the necessary medical aids.
- grossly inadequate housing or homelessness.
- inadequate medical care, not taking prescribed medications properly.

Exploitation

- sudden changes in bank account or banking practice, including an unexplained withdrawal of large sums of money.
- adding additional names on bank signature cards.
- unauthorized withdrawal of funds using an ATM card.
- abrupt changes in a will or other financial documents.
- unexplained disappearance of funds or valuable possessions.
- bills unpaid despite the money being available to pay them.
- forging a signature on financial transactions or for the titles of possessions.
- sudden appearance of previously uninvolved relatives claiming rights to a vulnerable adult’s possessions.
- unexplained sudden transfer of assets to a family member or someone outside the family.
- providing services that are not necessary.
- individual's report of exploitation.

Version Control - Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	February 23	Initial draft approved	Annually
2.0	CEO	October 23	Reviewed and updated	

This policy will be reviewed as part of any safeguarding incident investigation, to test that it has been complied with and to see if any improvements might realistically be made to it.

Statutory Guidance

Gov.UK – The role of other agencies in safeguarding
CC: Infographic; 10 actions trustees need to take.
CC: Safeguarding duties of charity trustees
CC: Safeguarding - policies and procedures
CC: How to protect vulnerable groups
CC: Managing online risk.