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 appropriatemeasures can then be taken to preserve confidentiality. If you are in any doubt, you can seekadvice from the Citizens Advice or ACAS, or Protect, the independent whistleblowingcharity, who offer a confidential helpline. 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:

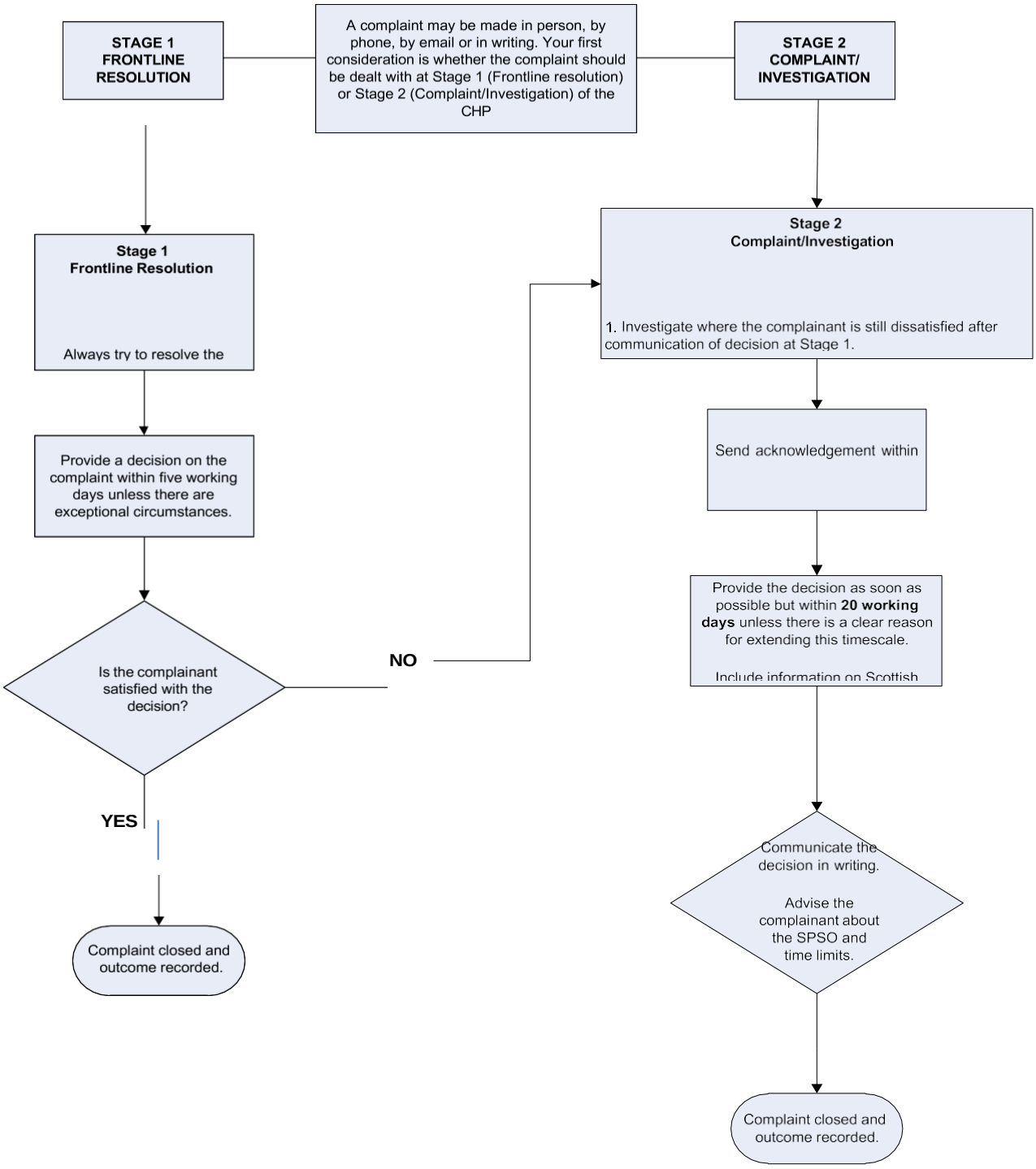
a. Submitting a Written Complaint: The learner should submit a written complaint, detailing the nature of the complaint, including any relevant dates, times, and individuals involved. This written complaint should be addressed to the complaints officer or relevant designated contact person.

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.