Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Review Sheet

Last Reviewed	Last Amended	Next Planned Review
30 Mar '21	30 Mar '21	in 12 months, or sooner as required.

Business impact	HIGH IMPACT — These changes require action as soon as possible.
Reason for this review	Scheduled review
Were changes made?	Yes
Summary:	This policy focuses on the Data Security and Protection Toolkit and provides a guide to services on how this should be completed. It has been reviewed to now include information on the 'Approaching Standards' which came into force on 5th March 2021. The policy content has been updated throughout to reflect this change including the ongoing changes in the structure and development of the tool. New references from Digital Social Care have also been added and existing ones updated to ensure they remain current.
Relevant legislation:	• The Care Act 2014 • The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 • Data Protection Act 2018 • UK GDPR
Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: Digital Social Care, (2021), *Completing Standards Met - How to Guide*. [Online] Available from: https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/04/Standards-Met-Guide-v.-9.pdf [Accessed: 30/3/2021] • Author: Digital Social Care, (2021), *Completing Approaching Standards on the Data Security and Protection Toolkit - How to Guide*. [Online] Available from: https://www.digitalsocialcare.co.uk/latest-guidance/completing-approaching-standards/ [Accessed: 30/3/2021] • Author: Digital Social Care, (2019), *Data Security and Protection Toolkit: 'Standards Met' Guidance for Social Care Providers*. [Online] Available from: https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/06/DSPTStandardsMetGuideASC_v4.pdf [Accessed: 30/3/2021] • Author: NHS Digital, (2021), *Data Security and Protection Toolkit*. [Online] Available from: https://www.dsptoolkit.nhs.uk/ [Accessed: 30/3/2021]
Suggested action:	• Encourage sharing the policy through the use of the QCS App • Widely distribute the 'Key Facts' of the policy
Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

1. Purpose

1.1 This policy will highlight the steps required in order for Henry Nihill House to comply with the Data Security and Protection (DSP) Toolkit.
1.2 To enhance our suite of Policies that cover Data Protection, Cyber Security and general UK GDPR compliance. As well as providing a social care perspective for Henry Nihill House on information governance, it will provide best practice principles through the Data Security and Protection Toolkit (DSPT) in order to demonstrate what needs to be part of Henry Nihill House culture in order to continue to receive NHS contracts.
1.3 The policy will provide guidance on how to access the Data Security and Protection Toolkit, and will act as a guide and signpost Henry Nihill House to available resources.
1.4 To support Henry Nihill House in meeting the following Key Lines of Enquiry:

Key Question	Key Lines of Enquiry
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?
WELL-LED	W5: How does the service work in partnership with other agencies?

1.5 To meet the legal requirements of the regulated activities that {Henry Nihill House} is registered to provide:

- The Care Act 2014
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Data Protection Act 2018
- UK GDPR

2. Scope

2.1 The following roles may be affected by this policy:

- Registered Manager
- Other management
- Administrator

2.2 The following Service Users may be affected by this policy:

- Service Users

2.3 The following stakeholders may be affected by this policy:

- Commissioners
- Local Authority
- NHS

3. Objectives

3.1 To raise awareness and competency within Henry Nihill House around the requirements of the Data Security and Protection Toolkit:

- To ensure that those with role-specific duties are aware of how this affects their role
- To ensure that, where required, those with specific roles and requirements receive appropriate training
- To ensure that all staff receive induction and ongoing training with regards to Data Security and Cyber Protection
- To ensure safe, secure data sharing with the NHS

3.2 To ensure that there is a clear Data Security and Protection Toolkit 'roadmap' for Henry Nihill House, using:

- Guidance and Templates for meeting the Ten Standards
- Templates for audit and spot checks
- A checklist for home workers to ensure compliance

4. Policy

4.1 The Data Security and Protection Toolkit is an online self-assessment tool that Henry Nihill House and all social care providers must use if they have access to NHS patient data and systems.
As a result of this requirement, Henry Nihill House recognises the importance of data security and cyber protection and is committed to maintaining systems that support confidentiality and the wider understanding of how data must be managed.
There are two stages on the pathway:

- Approaching Standards
- Standards Met

4.2 The Data Security and Protection Toolkit allows Henry Nihill House to measure its performance against the National Data Guardian's 10 Data Security Standards, which are:

- **Standard 1:**
  - All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
- **Standard 2:**
  - All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches
- **Standard 3:**
  - All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit
- **Standard 4:**
  - Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals
- **Standard 5:**
  - Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security
- **Standard 6:**
  - Cyber attacks against services are identified and resisted. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection
- **Standard 7:**
  - A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management
- **Standard 8:**
  - No unsupported operating systems, software or Internet browsers are used within the IT estate
- **Standard 9:**
  - A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually
- **Standard 10:**
  - IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards

4.3 If Henry Nihill House does not provide care through the NHS Standard Contract, there is no required action to take.
However, it is recommended that all social care providers consider compliance with the new Data Security and Protection (DSP) Toolkit.

This will help to demonstrate best practice and ensure compliance with the 10 Data Security Standards.
4.4 The CQC includes a focus on the use of technology and sharing information for the benefit of the care to the individual.
Whilst the prompts under KLOE W2 do not specifically reference the Data Security and Protection (DSP) Toolkit, it details that providers should operate within a framework that demonstrates robust arrangements around the security, availability, sharing and integrity of confidential data, records and data management standards.
4.5 It has been recognised that social care services such as Henry Nihill House can be very different to health services, and this has been reflected in the revised approach to the Data Security and Protection (DSP) Toolkit for social care.
The requirements for Social Care have been broken down in to four key areas within the DSPT.

- Staffing and Roles
- Policies and Procedures
- Data Security
- IT Systems and Devices

Each category will have a subset of requirements that, once completed, will enable Henry Nihill House to achieve "Standards Met" status.

4.6 Meeting the Standards

The 'Approaching Standards' status was introduced as a new status available to care providers who have demonstrated good progress but have not yet reached 'Standards Met'.

- Henry Nihill House will review its self-assessment and follow the actions to take in relation to the new Approaching Standards Assessment
- Where required, Henry Nihill House can also refer to the Digital Social Care website for help and support
- The next level is evidencing compliance with 'Standards Met'

The Data Security and Protection Toolkit: Standards Met Guidance for Social Care Providers will help any providers who are working towards achieving ‘Standards Met’.
4.7 This policy and wider data security management are supported by the comprehensive range of data protection policies, templates and guidance that are available within the QCS Management System.
This Data Security and Protection (DSP) policy will support Henry Nihill House in understanding responsibilities with regard to data management and security. When the Toolkit is completed, it will support compliance with data protection requirements, and add to Henry Nihill House assurances regarding:

- Confidentiality
- Data Protection
- Cyber Security
- Information Governance
- Staff Training

In addition, it will provide supporting evidence towards meeting the CQC KLOEs.

5. Procedure

5.1 Compliance with the Standards

Within the forms section of this policy, the following tools are included:

- DSPT Operational Audit
- Spot Check Audit
- Home Working Checklist
- DSPT Action Planning Form

Using these tools ahead of registering with the DSPT will enable Catherine Palmer or a delegated team member to gain an understanding of the requirements and where Henry Nihill House is positioned at the start of the registration process.

The tools will also provide evidence towards compliance and best practice as they are designed to support with ongoing monitoring.

5.2 When the DSPT Needs to be Completed

Due to the coronavirus pandemic, the deadline for the 2020-2021 publication is 30 June 2021.

The DSP Toolkit usually runs from 1 April to 31 March and needs to be completed annually.

5.3 Before Registering

Henry Nihill House will need to source an Organisational Data Service (ODS) Code, which is created from CQC data. Where there are any issues with the data held by ODS, this will mean the CQC also has incorrect data.

Any corrections (such as to an address) will need to be made to the CQC and any changes will flow to ODS.

All care home and domiciliary providers will have at least two codes, an HQ code ("parent code") and a one or more sites code ("child code").

If a number of codes come up on the search and you do not know the correct one, you can read guidance here on the codes; or you can contact Digital Social care via 0208 133 3430 (Mon-Fri 9-5), or help@digitalsocialcare.co.uk.

5.4 Registration

Henry Nihill House will then register with the DSPT at https://www.dsptoolkit.nhs.uk/Account/Register, and follow the prompts to complete registration.

5.5 Completing the Profile of Henry Nihill House

Once registered, Henry Nihill House will need to sign in, in order to complete the profile.

1. Go to https://www.dsptoolkit.nhs.uk/Account/Login.
2. To sign in for the first time, click on the 'Forgot your Password' button. This will enable the setting of an Administrator password.
3. Once signed in, click on the 'Continue to Questions' button to complete the profile of Henry Nihill House.
4. Choose an organisation type. Select "social care".
5. A list of voluntarily questions will appear. It is best practice to fill in who has the following roles in Henry Nihill House:
   - Caldicott Guardian
   - Senior Information Risk Owner (SIRO)
   - Information Governance Lead
   - Data Protection Officer (DPO)
6. If Henry Nihill House has gained access to NHSmail or has a Cyber Essentials Plus certification, select the right option, or select 'Not Sure'.
7. Once the information has been uploaded and checked, 'Accept and Submit'.
8. Changes can be made at any point in the process using the navigation tabs.

5.6 Setting Up Other Users for Henry Nihill House

Certain roles within Henry Nihill House might share work on the DSP Toolkit.

Using the administrator account allows the addition of more users and assigning access levels.

To do this:

1. Sign in to the DSP Toolkit and click on the 'Admin' tab on the top right-hand corner of the page. This will reveal a drop-down list.
2. Select 'User List'.

3. Once on the 'User List' page, additional users can be added.
Users can be allocated one of three roles:

- **Auditor:**
  - Will be able to view assertions/evidence/organisation profile, reset own password and update own personal details
- **Member:**
  - Will be able to view assertions, view/add/edit evidence, view organisation profile (but not edit), reset own password and update own personal details
- **Administrator Member:**
  - Will be able to view and confirm assertions, view/add/edit evidence, allocate assertion owners, submit and publish assessment, view and edit organisation profile, create and edit users for Henry Nihill House, reset own password and update own personal details

5.7 Approaching and Meeting the Standards

The DSP Toolkit is organised in relation to the 10 Data Security Standards under four groups:

- Staffing and Roles
- Policies and Procedures
- Data Security
- IT Systems and Devices

There are 27 mandatory questions which need to be completed to achieve the 'Approaching Standards' status.
Once 'Approaching Standards' has been met, the remaining 18 questions will need to be completed to achieve the 'Standards Met' status.
There is no specific order to completing the DSP Toolkit, you can start anywhere and go back and forth between the evidence items.
Where QCS data protection policies, templates and guidance have been fully adopted by Henry Nihill House and all items have been completed, Henry Nihill House will be able to provide evidence to meet the required 'Approaching Standards' and 'Standards Met' by using the QCS tools provided.

5.8 Publishing the Assessment of Henry Nihill House

Only Administrator Members can publish assessments.
On completion of all of the ‘Approaching Standards’ or 'Standards Met' requirements, the DSPT will prompt an assessment to be published:

- Click on the 'Publish Approaching Standards Assessment' button
- For any actions required, the system will offer to download an action plan template
- The blank action plan template will list the requirements that have not been responded to (if applicable). It should be completed and uploaded before publishing the assessment
- Click on the 'Publish Approaching Standards Assessment' button
- The DSP Toolkit requires confirmation from the publisher that Henry Nihill House is happy to continue and the organisation details are correct
- Click the 'Continue with Publication' button
- Once complete, Henry Nihill House will receive an email and screen confirmation that the submission has been published
- After publication, work can still continue on the assessment if necessary

5.9 Finding Help

To help Henry Nihill House with compliance, the Digital Social Care website has a dedicated section to support organisations.
This is a clear document that will add to the content of this policy. It will assist Henry Nihill House with the purpose and guide with the completion of the DSP Toolkit.
If Henry Nihill House is having technical difficulties with any part of the DSP Toolkit, please contact the DSP Toolkit team, and if there are any concerns or questions about the process please contact: ig.feedback@careprovideralliance.org.uk.
There are 'big picture guides' that give a broader view of the 10 Data Security Standards available here: https://www.dsptoolkit.nhs.uk/Help/23.

The Data Security and Protection Toolkit: Standards Met Guidance for Social Care Providers will offer additional guidance if required.

6. Definitions

6.1 DSP Toolkit

- The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 Data Security Standards
- All organisations that have access to NHS patient data and systems must use the DSP Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly

6.2 Caldicott Guardian

- A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure that it is used properly. All NHS organisations and local authorities that provide social services must have a Caldicott Guardian

6.3 Organisational Data Service Code

- An ODS code (also called an Organisation Code) is a unique code created by the Organisation Data Service within NHS Digital, and used to identify organisations across health and social care. ODS codes are required in order to gain access to national systems like NHSmail and the Data Security and Protection Toolkit (DSPT)

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- There is an increased recognition that social care requirements with regard to data security are different from health services
- The Care Provider Alliance, Department of Health and Social Care and the NHS have produced new guidance and materials to support completion of the DSP Toolkit
- Only providers providing services under NHS contracts are required to complete the DSP Toolkit, although the DSP Toolkit reflects good practice
- The simpler 'Approaching Standards' requirements will allow access to NHSmail to be a step on the road to full compliance
- After 'Approaching Standards', providers can progress on to 'Standards Met' level of compliance
- The DSP Toolkit is an online self-assessment and needs to be submitted annually
- Forms are provided within the policy to show what is required and promote the use of an action plan to address concerns or shortfalls in evidence
- The wider GDPR policies, templates and guidance will provide evidence and support completion of the toolkit

Key Facts - People affected by the service

People affected by this service should be aware of the following:

- We take your data protection seriously within Henry Nihill House and have a suite of policies and tools in place to ensure we fully comply with legislation and best practice
- We will ensure that we meet minimum standards of expected practice with data protection and security
- If you would like to further discuss how we ensure your data is protected, please discuss this with the Registered Manager

Further Reading

There is no further reading for this policy, but we recommend the 'underpinning knowledge' section of the review sheet to increase your knowledge and understanding.

Outstanding Practice

To be ‘ outstanding ’ in this policy area you could provide evidence that:

- The wide understanding of the policy is enabled by proactive use of the QCS App
- The 'Standards Met' level of compliance is achieved
- GDPR policies and procedures are fully embedded into practice at Henry Nihill House
- There have been no breaches of data security, and measures are in place to restrict the possibility of breaches occurring
- Data security and protection are included as a standing item in team and management meetings
- Data security and protection is widely understood at Henry Nihill House

Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
DSP Toolkit - Achieving Standards/Meeting Standards, Action Planning - AB37	To confirm compliance and identify areas for action.	QCS
Confidentiality and Data Protection Monitoring/Spot Check Audit - AB37	To evidence that data protection spot checks have been completed.	QCS
General Data Security Operational Audit - AB37	To ensure that all general data security checks have been completed within the service.	QCS
Data Security Checklist - Working from Home - AB37	For staff to complete when working from home.	QCS

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Approaching DSPT Standards Audit / Action Plan

The Data Security and Protection (DSP) Toolkit allows social care providers to measure performance against the National Data Guardian's 10 Data Security Standards, which are:

Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Standard 3: All staff complete appropriate annual data security training and pass a mandatory test provided through the revised Information Governance Toolkit.

Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Standard 6: Cyber attacks against services are identified and resisted. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Standard 8: No unsupported operating systems, software or Internet browsers are used within the IT estate.

Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

In order to achieve 'Approaching Standards' or 'Standards Met' status you must complete the DSPT online tool.

The following Audit/Action Plan contains all the mandatory elements required that allows you to gather evidence prior to completing the online tool. Completing all sections highlighted in Green will enable you to achieve 'Approaching Standards' status. Completing all of the additional sections highlighted in Blue will enable you to achieve 'Standards Met' status.

The DSPT has now been divided into sections. Evidence items are now numbered and organised under four headings:

- Staffing and roles
- Policies and procedures
- Data security
- IT systems and devices

Voluntary Questions on the DSPT

Who holds the roles of	**Action Needed**		**If Yes, What Action?**	**By Who?**	**By When?**
	Yes	**No**			
Caldicott Guardian					
Senior Information Risk Owner					
Information Governance Lead					
Data Protection Officer					

Section 1	**Staffing & Roles**

Standard 1 **Evidence**	**Action Needed**		**If Yes, What Action?**	**By Who?**	**By When?**
	Yes	**No**			
1.1.2. Who has responsibility for data security and protection and how has this responsibility been formally assigned?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Standard 2 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
2.2.1. Does your organisation have an induction process that covers data security and protection, and cyber security?					
2.2.2. Do all employment contracts, and volunteer agreements, contain data security requirements?					

Standard 3 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed in the last 12 months?					
3.2.1 Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, within the last 12 months?					
3.4.1 Have the people with responsibility for data security and protection received training suitable for their role?					

Standard 4 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Section 2	Policies & Procedures

Standard 1 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
1.2.1 Does your organisation have up to date policies in place for data protection and for data and cyber security?					
1.3.1 What is your organisation's information Commissioner's Office (ICO) registration number?					
1.3.2 Does your organisation have a privacy notice(s)					
1.4.1 Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?					
1.4.4 Is your organisation compliant with the national data opt-out policy?					
1.5.2 Does your organisation carry out regular data protection spot checks?					
1.6.1 Does your organisation's data protection policy describe how you keep personal data safe and secure?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Standard 1 (Cont) Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
1.6.5 Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?					
1.7.2 If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed within the last 12 months? This contract should meet the requirements set out in data protection regulations.					
1.7.3 If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?					
1.7.4 Does your organisation have a timetable which sets out how long you retain records for?					

Standard 10 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
10.1.2 Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Section 3	Data Security

Standard 1 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
1.6.2 How does your organisation make sure that paper records are safe when taken out of the building?					
1.6.3 Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.					

Standard 5 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
5.1.1 If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?					

Standard 6 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
6.1.1 A data security and protection breach reporting system is in place.					
6.1.4 If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?					
6.1.5 If your organisation has had a data breach, were all individuals who were affected informed?					

Standard 7 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
7.1.2 Does your organisation have a business continuity plan that covers data and cyber security?					
7.2.1 How does your organisation test the data and cyber security aspects of its business continuity plan?					

Section 4	IT Systems and Devices

Standard 1 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
1.6.4 What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?					
1.6.6 If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?					
1.8.3 What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?					

Standard 4 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
4.1.2 Does your organisation know who has access to personal and confidential data through its IT system(s)?					

Standard 4 (Cont) Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
4.2.5 Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?					
4.3.1 Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?					
4.5.4 How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?					

Standard 6 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
6.2.3 Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?					
6.3.2 Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?					

Standard 7 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
7.3.1 How does your organisation make sure that there are working backups of all important data and information?					
7.3.2 All emergency contacts are kept securely, in hardcopy and are up-to-date.					

Standard 7 (Cont) **Evidence**	**Action Needed**		**If Yes, What Action?**	**By Who?**	**By When?**
	Yes	**No**			
7.3.4 Are backups routinely tested to make sure that data and information can be restored?					

Standard 8 **Evidence**	**Action Needed**		**If Yes, What Action?**	**By Who?**	**By When?**
	Yes	**No**			
8.1.4 Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?					
8.2.1 If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.					
8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Standard 9 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
9.1.1 Does your organisation make sure that the passwords of all networking component, such as a Wi-Fi router, have been changed from their original passwords?					
9.6.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?					

Standard 10 Evidence	Action Needed		If Yes, What Action?	By Who?	By When?
	Yes	No			
10.2.1 Do your organisation's IT system suppliers have cyber security certification?					

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Outcome		Scoring	Rationale
Maximum Audit Score:			Many significant shortcomings
Achieved Audit Score:		**2**	Shortcomings outweigh good practice
Auditor Name:		**3**	Minimum acceptable standard
Signed:		**4**	Good practice outweighs shortcomings
Date of Audit:			No significant shortcomings
Assessors in order to be assured of compliance. Evidence must be observed where possible that systems and process' are clearly followed as outlined in Policies and Procedures.			

Staffing			**Further Actions Yes/No/N/A**
Question	**Score**	**Rationale**	
After discussion with staff. Do they understand their responsibility towards data security?			
After discussion with staff. Are they aware of our data protection policies?			
Have staff received training on data protection?			
Have any staff undergone disciplinary action in relation to data protection and security?			
Spot check that staff understand how to report security breaches and near misses.			

Physical Access to hardcopy records			**Further Actions Yes/No/N/A**
Question	**Score**	**Rationale**	
Check records of which staff have access to confidential areas is up to date.			
Are offices, files, cabinets that contain confidential information kept locked when not in use?			
Has confidential waste been disposed of securely, are there destruction certificates?			
Has anyone inappropriately accessed, or attempted to access, confidential records?			
There are access agreements in place to allow access to confidential files?			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Digital Access to records			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Is the allocation of administrator rights restricted?			
Have staff access rights been reviewed?			
Check if there is any evidence of staff sharing access rights.			
Screens are locked when not in use.			
Check that our password policy is being followed.			
Has anyone inappropriately accessed, or attempted to access, confidential records?			
Are appropriate security measures applied to computers, laptops, mobiles etc?			
Staff are using computers appropriately and in line with policies and procedures?			

Sharing Data			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Our procedures for safely sharing personal information via post are being followed.			
Our procedures for safely sharing personal information via fax are being followed.			
Our procedures for safely sharing personal information via secure email are being followed.			

Legal Checks			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
The Information Asset Register has been reviewed and signed off.			
The Record of Processing Activities has been reviewed and signed off.			
Records of consent are up to date and still applicable.			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Audit Action Plan				
Issue	**Action Required**	**By Who**	**By When**	**Completed**

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Outcome		**Scoring**	**Rationale**
Maximum Audit Score:	250		Many significant shortcomings
Achieved Audit Score:		**2**	Shortcomings outweigh good practice
Auditor Name:		**3**	Minimum acceptable standard
Signed:		**4**	Good practice outweighs shortcomings
Date of Audit:			No significant shortcomings
Assessors in order to be assured of compliance. Evidence must be observed where possible that systems and process' are clearly followed as outlined in Policies and Procedures.			

General Policies & Practices			**Further Actions Yes/No/N/A**
Question	**Score**	**Rationale**	
An up-to-date policy and procedure is in place for data protection, data and cyber security?			
Data security direction set at management level and translated into effective practices?			
A named person responsible for data security, protection is within policies and procedures?			
The policy and procedures are compliant with the national data opt-out policy?			
The policies and procedures have an up-to-date list of how data is held and shared for different types of personal and sensitive information?			
There is evidence of regular data protection spot checks?			
The Data Protection Policy and Procedure describes how personal data is kept safe and secure?			
The business continuity plan contains data and cyber security?			
There are tests on aspects of the business continuity plan around data and cyber security?			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Sharing Data			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Data security and protection policies are available to the public?			
The policy and procedure for paper records details how these are kept safe when taken out of the building? e.g. in a Service User's own home			
A central record is held on who has access to personal, confidential data through use of IT?			

Managing Risk			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Physical controls are in place that prevent unauthorised access to personal data, e.g. locked doors, cabinets, rooms, etc.			
The data protection policies describe how risks to personal data are identified and minimised when introducing or changing a process, or starting new systems involving personal data?			
The top three data and cyber security risks are identified and a plan to reduce those risks is contained in policies & procedures incl. Business Continuity planning?			
There is a policy and procedure in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?			
There is a policy and procedure in place for when anyone connected with the business uses their own devices (e.g. phones) for work purposes?			
All emergency contacts are kept securely, in hardcopy and are up to date.			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Records			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
There is a policy and procedure in place that details a timetable which sets out how long records are retained?			
Is a third party used to destroy records or equipment that hold personal data; is there a written contract in place that has been reviewed since 1st April 2020?			
The above contract meets the requirements set out in data protection regulations?			
Employment contracts and volunteer agreements contain data security requirements?			

Staffing			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
The induction process covers data security and protection, and cyber security?			
The induction and ongoing training process covers General Data Protection Regulations?			
A training needs analysis covering data security and protection, and cyber security, is in place?			
Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1 April 2020?			
Have the people with responsibility for data security and protection received training suitable for their role?			
Does your organisation have an up-to-date record of staff, and volunteers if you have them, and their roles?			
The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Staffing			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Have you observed staff, directors, trustees and volunteers use good password practice?			
Have all staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe as per policy?			

Data Breaches			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Does the policy and procedure highlight a system/process to report data breaches?			
Has a data breach or a near miss occurred in the last year?			
If yes, has a 'lessons learnt' exercise been carried out of the incident that may have allowed the breach to occur?			
If yes, was the senior management team notified, and did they approve the actions planned to minimise the risk of a recurrence?			
If a data breach has occurred, were all individuals who were affected informed?			
Do all the computers and other devices used have antivirus/antimalware software which is kept up to date?			
Is there an IT process in place to make sure that there are working backups of all important data and information?			

Information Technology Systems			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
A central record is held on who has access to personal, confidential data through use of IT?			
IT administrators have a reliable way of removing, amending access to IT systems when people leave or change roles?			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Information Technology Systems (Continued)			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
All the IT system's administrators have signed an agreement to hold them accountable to higher standards?			
The policies and procedures highlight the need for users to observe good password practice?			
Do all the computers and other devices used have antivirus/antimalware software which is kept up to date?			
There is an IT process in place to make sure that there are working backups of all important data and information?			
Are all the IT systems and the software used still supported by the manufacturer or the risks are understood and managed?			
IT systems and software not being supported by the manufacturer and software risks are being managed, a risk plan is in place summarising the risk of continuing to use each unsupported item, the reasons for doing so and a summary of action taken to minimise risk.			
The latest software updates are downloaded and installed appropriately by IT?			
Passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords and are changed periodically to reduce risk?			
A central record of suppliers that handle personal information, the products, services delivered, and contact details is held?			
A record is held of all IT system suppliers that have cyber security certification?			

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

Audit Action Plan				
Issue	**Action Required**	**By Who**	**By When**	**Completed**

Henry Nihill House
Henry Nihill house 94 Priory Field, EDGWARE, Middlesex, HA8 9PU

The layers of security relied on in the workplace are naturally reduced when working remotely; and the following declaration will help ensure our work and data remains effective and secure.

	Self-declaration	**Agreed & Understood**		
		Yes	**No**	**N/A**
1.	I am alert to COVID-19 phishing and vishing (telephone equivalent of phishing) scams. *(If in doubt, seek advice from the Registered Manager or the IT security team if something does not feel right, be it an email, a phone call, or a physical approach)*			
2.	I will not use public Wi-Fi, I will either work offline and connect later once at home on a more secure network or connect by tethering to my mobile device			
3.	I will be suspicious of any emails asking to check or renew my passwords and login credentials. *(Try to verify the authenticity of the request through other means e.g. call the IT helpdesk)*			
4.	I will not click on suspicious links or open any suspicious attachments			
5.	I have changed the admin/default password on my home broadband router			
6.	I have ensured the firmware on my home broadband router is up to date			
7.	I will make sure I am running all the latest versions of software on all my devices			
8.	I will password protect confidential documents that I send across the internet to other colleagues			
9.	I will not use my work email address to register on non-work-related websites			
10.	I have a data back-up strategy, and will remember to do it (All important files will be backed up regularly e.g. weekly)			
11.	I will always keep all my work devices with me when travelling. (never leave work laptops or devices in cars)			
12.	never allow anyone else such as family members to access my devices for personal use such as internet browsing			
13.	I will reduce paper-handling to zero. *(Do not print documents and work on them in public spaces. They will be vulnerable to theft or misplacement)*			
14.	All paper documents no longer needed will be disposed of in a secure manner. *(Use a cross-cut or micro-cut shredder)*			
15.	I use a screen protector to prevent shoulder surfing if I am in a public space or in shared accommodation			
16.	I do not write passwords down.			
17.	I keep my work telephone conversations and online meetings discreet. *(Hold them in a private place if possible)*			
18.	I never leave equipment unattended, anywhere. *(It is good behavioural practice to lock the workstation when away from it at home and, if in shared accommodation, it is obligatory)*			
19.	I have familiarised myself with the accident and incident reporting policy and procedure and will report any incidents as soon as I become aware of them			

Name:		**Job Role:**	
Signature:		**Date:**	