Review Sheet

Last Reviewed
28 Nov '23

Last Amended
28 Nov '23

Next Planned Review in 12 months, or sooner as required.

Business impact	**MEDIUM IMPACT** Changes are important, but urgent implementation is not required, incorporate into your existing workflow.
Reason for this review	Scheduled review
Were changes made?	Yes
Summary:	This policy remains focused on the Data Security and Protection Toolkit and provides a guide to services on how this should be completed. It has been reviewed with some minor policy changes and updates. Underpinning Knowledge and Further Reading links have been reviewed to ensure the most up to date information remains available with additional sources of information and guidance added.
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: UK Caldicott Guardian Council, (2023), *Resources and Guidance Pages*. [Online] Available from: https://www.ukcgc.uk/ [Accessed: 28/11/2023] • Author: Information Commissioner's office, (2022), *Guidance and Resources*. [Online] Available from: https://ico.org.uk/ [Accessed: 28/11/2023] • Author: NHS, (2023), *National data opt-out*. [Online] Available from: https://digital.nhs.uk/services/national-data-opt-out [Accessed: 28/11/2023] • Author: Digital Care Hub, (2023), *The Data Security and Protection Toolkit*. [Online] Available from: https://www.digitalcarehub.co.uk/dspt/ [Accessed: 29/5/2024] • Author: NHS Digital, (2023), *Data Security and Protection Toolkit*. [Online] Available from: https://www.dsptoolkit.nhs.uk/ [Accessed: 28/11/2023] • Author: CQC, (2023), *Regulation 17: Good Governance*. [Online] Available from: https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-17-good-governance [Accessed: 28/11/2023]
Suggested action:	• Encourage sharing the policy through the use of the QCS App
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.

1. Purpose

1.1 This policy will highlight the steps required in order for Generations Care Ltd to comply with the Data Security and Protection Toolkit (DSPT) if and when applicable.
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 Generations Care Ltd 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 Generations Care Ltd 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 Generations Care Ltd to available resources.

1.4 To support Generations Care Ltd in meeting the following Key Lines of Enquiry/Quality Statements (New):

Key Question	Key Lines of Enquiry	Quality Statements (New)
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?	QSW5: Governance, management and sustainability
WELL-LED	W5: How does the service work in partnership with other agencies?	QSW6: Partnerships and communities

1.5 To meet the legal requirements of the regulated activities that Generations Care Ltd 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 Generations Care Ltd 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 Generations Care Ltd, using:

- Guidance and templates for meeting the required ten standards
- Templates for audit and spot checks
- A checklist for those working from home to ensure compliance

4. Policy

4.1 The Data Security and Protection Toolkit is an online self-assessment tool that Generations Care Ltd and all social care providers must use if they have access to NHS patient data and systems.
As a result of this requirement, Generations Care Ltd 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 three stages on the pathway:

- **Approaching Standards**
  - This is the minimal legal standard
  - An action plan is required with this standard
  - Generations Care Ltd will gain access to NHS Mail
- **Standards Met**
  - Sets Generations Care Ltd above legal requirements
  - Gives reassurance of the data and cyber security of Generations Care Ltd
  - Helps to answer CQC Questions
- **Standards Exceeded**
  - For example, Generations Care Ltd may have Cyber Essentials PLUS

4.2 The Data Security and Protection Toolkit allows Generations Care Ltd to measure its performance against the National Data Guardian’s 10 Data Security Standards. The standards are organised under 3 leadership obligations which are:
People
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

- **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

Process
Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

- **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 data 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 and Care CERT security advice is responded to. Action is taken immediately following a data breach, also known as 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

Technology
Ensure technology is secure and up to date.

- **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 Generations Care Ltd 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 Care Quality Commission includes a focus on the use of technology and sharing information for the benefit of the Care to the individual.
Whilst the CQC prompts do not specifically reference the Data Security and Protection Toolkit (DSPT), they detail 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.
In November 2021, CQC introduced additional prompts that included information governance / use of technology, they include:

- Effective
  - How is technology and equipment used to enhance the delivery of effective care and treatment and to support people’s independence
- Responsive
  - How is technology used to support people to receive care and support quickly? Is the technology easy to use?
- Well-led
  - Are information technology systems used effectively to monitor and improve quality of care?
- Well-led
  - Does the service share appropriate information and assessments with other relevant agencies for the benefit of people who use the service?

4.5 It has been recognised that social care services such as Generations Care Ltd can be very different to health services, and this has been reflected in the revised approach to the Data Security and Protection Toolkit (DSPT) 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 Generations Care Ltd to achieve "Standards Met" status.
4.6 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 Compliance Centre.
This Data Security and Protection Toolkit (DSPT) Policy and Procedure will support Generations Care Ltd 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 assurance

for Generations Care Ltd regarding:

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

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

5. Procedure

5.1 Compliance with the Standards

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

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

Using these tools ahead of registering with the DSPT will enable Mr Victor Rivete or a delegated team member to gain an understanding of the requirements and where Generations Care Ltd 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.

Digital Care Hub also provides useful tools and resources.

5.2 When the DSPT Needs to be Completed

The DSPT needs to be completed annually in line with the requirements published here.

5.3 Before Registering

Generations Care Ltd 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

Generations Care Ltd 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 Generations Care Ltd

Once registered, Generations Care Ltd 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 Generations Care Ltd.

4. Choose an organisation type. Select "social care".

5. A list of voluntary questions will appear. It is best practice to fill in who has the following roles in Generations Care Ltd:

- Caldicott Guardian
- Senior Information Risk Owner (SIRO)
- Information Governance Lead
- Data Protection Officer (DPO)

6. If Generations Care Ltd 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 Caldicott Guardian

All health and adult social care bodies in England must have a Caldicott Guardian in place from 30 June 2023. Please refer to the Caldicott Guardian Policy and Procedure.

5.7 Setting Up Other Users for Generations Care Ltd

Certain roles within Generations Care Ltd might share work on the DSPT.

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

To do this:

1. Sign in to the DSPT 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 Generations Care Ltd, reset own password and update own personal details

5.8 Approaching and Meeting the Standards

The DSPT 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 a number of mandatory questions which need to be completed to achieve ‘Approaching Standards’ status.

Once ‘Approaching Standards’ has been met, the remaining questions will need to be completed to achieve the ‘Standards Met’ status.

Standards Exceeded

If Generations Care Ltd has achieved 'Standards Met' and also a Cyber Essentials PLUS certification recorded in its Organisation Profile, then its status will be displayed as 'Standards Exceeded'.

There is no specific order to completing the DSPT, 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 Generations Care Ltd and all items have been completed, Generations Care Ltd will be able to provide evidence to meet the required 'Approaching Standards' and 'Standards Met' by using the QCS tools provided.

5.9 Publishing the Assessment of Generations Care Ltd

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 DSPT requires confirmation from the publisher that Generations Care Ltd is happy to continue and the organisation details are correct

- Click the 'Continue with Publication' button
- Once complete, Generations Care Ltd will receive an email and screen confirmation that the submission has been published
- After publication, work can still continue on the assessment if necessary

5.10 Annual Review

Where required to do so, Generations Care Ltd will review its DSPT submissions annually. This process will include

- Reviewing and updating existing answers on the system
- Completing ALL mandatory questions to get to standards met
- Confirm and assert all submitted answers
- Publish the results

5.11 Finding Help

To help Generations Care Ltd 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 Generations Care Ltd with the purpose and guide with the completion of the DSPT.

If Generations Care Ltd is having technical difficulties with any part of the DSPT, please contact the DSPT 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 Data Security and Protection Toolkit (DSPT)

- 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 DSPT 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)

6.4 National Data Opt-out

- The National Data Opt-out is a service that allows Service Users to opt out of their confidential (patient) Service User information being used for research and planning.

6.5 Information Commissioner’s Office

- The ICO is the UK's independent body set up to uphold information rights

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 DSPT
- Only providers providing services under NHS contracts are required to complete the DSPT, although the DSPT 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 wider GDPR policies, templates and guidance will provide evidence and support completion of the toolkit
- The DSPT 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

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 Generations Care Ltd 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

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

GOV.UK - National Data Guardian guidance on the appointment of Caldicott Guardians, their role and responsibilities:
https://www.gov.uk/government/publications/national-data-guardian-guidance-on-the-appointment-of-caldicott-guardians-their-role-and-responsibilities

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
- Data security and protection is widely understood at Generations Care Ltd
- GDPR policies and procedures are fully embedded into practice at Generations Care Ltd
- 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

Forms

The following forms are included as part of this policy:

Title of form	**When would the form be used?**	**Created by**
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

Data Security Spot Check			
Outcome		**Scoring**	**Rationale**
Maximum Audit Score:		**1**	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:		**5**	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?			
Have spot checks been carried out to see if staff understand how to report security breaches and near misses?			

Physical Access to hardcopy records			**Further Actions Yes/No/N/A**
Question	**Score**	**Rationale**	
Are the records of which staff have access to confidential areas 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?			
Are there access agreements in place to allow access to confidential files?			

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?			
Is there any evidence of staff sharing access rights?			
Are screens locked when not in use?			
Is our password policy being followed?			
Has anyone inappropriately accessed, or attempted to access, confidential records?			
Are appropriate security measures applied to computers, laptops, mobiles? (list not exhaustive)			
Are staff using computers appropriately and in line with policies and procedures?			

Sharing Data			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Are our procedures for safely sharing personal information via post being followed?			
Are our procedures for safely sharing personal information via fax being followed?			
Are our procedures for safely sharing personal information via secure email being followed?			
Are our procedures for complying with the National Data Opt out being followed?			

Legal Checks			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Has the Information Asset Register been reviewed and signed off?			
Has the Record of Processing Activities been reviewed and signed off?			
Are records of consent up to date and still applicable?			

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

Data Security Audit			
Outcome		**Scoring**	**Rationale**
Maximum Audit Score:	250	1	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:		5	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**	
Is there an up-to-date policy and procedure in place for data protection, data and cyber security?			
Is the data security direction set at management level and translated into effective practices?			
Is there a named person responsible for data security and protection within policies and procedures?			
Are the policies and procedures compliant with the national data opt-out policy?			
Do 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?			
Is there evidence of regular data protection spot checks?			
Does the Data Protection Policy and Procedure describe how personal data is kept safe and secure?			
Does the business continuity plan contain data and cyber security?			
Are there tests on aspects of the business continuity plan around data and cyber security?			

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

Managing Risk			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Are physical controls in place that prevent unauthorised access to personal data, e.g. locked doors, cabinets, rooms?			
Do 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?			
Are the top three data and cyber security risks identified and is there a plan to reduce those risks contained in policies and procedures including business continuity planning?			
Is there a policy and procedure in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?			
Is there a policy and procedure in place for when anyone connected with the business uses their own devices (e.g. phones) for work purposes?			
Are all emergency contacts kept securely in hardcopy, and are they up to date?			

Records			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Is there 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?			
Does the above contract meet the requirements set out in data protection regulations?			
Do employment contracts and volunteer agreements contain data security requirements?			

Staffing			Further Actions Yes/No/N/A
Question	**Score**	**Rationale**	
Does the induction process cover data security and protection, and cyber security?			
Does the induction and ongoing training process cover the UK General Data Protection Regulation?			
Is there a training needs analysis covering data security and protection, and cyber security, 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?			
Are the results of staff awareness surveys on staff's understanding of data security reviewed to improve data security?			

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 the 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	
Is a central record held on who has access to personal, confidential data through the use of IT?			
Do IT administrators have a reliable way of removing/amending access to IT systems when people leave or change roles?			

Information Technology Systems (Continued)			Further Actions Yes/No/N/A
Question	Score	Rationale	
Have all the IT system's administrators signed an agreement to hold them accountable to higher standards?			
Do 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?			
Is there 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 are the risks understood and managed?			
Where IT systems and software are not being supported by the manufacturer and software risks are being managed, is there a risk plan 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.			
Are the latest software updates downloaded and installed appropriately by IT?			
Have passwords of all networking components, such as a Wi-Fi router, been changed from their original passwords and are they changed periodically to reduce risk?			
Is there a central record of suppliers that handle personal information, the products, services delivered, and contact details held?			
Is there a record of all IT system suppliers that have cyber security certification held?			

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

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.	I 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:**	