Ref.	Question	Response	Comment
1.1.1	**Name of Senior Information Risk Owner.**	Tim Whalley	[not provided]
1.1.2	**SIRO Responsibility for data security has been assigned.**	Yes	[not provided]
1.1.3	**Name of Caldicott Guardian.**	N/A	No Caldicott Guardian has been appointed at this time
1.1.4	**Who are your staff with responsibility for data protection and/or security?**	Sylwia Indycka, Registered Manager Tim Whalley, Director Emma Abrew, HR Co-ordinator	[not provided]
1.1.5	**Staff awareness- Leadership (Q1) I feel data security and protection are important for my organisation.**	[not provided]	[not provided]
1.1.6	**Name of Appointed Data Protection Officer.**	N/A	No DPO has been appointed at this time
1.2.1	**There is a data security and protection policy or policies that follow relevant guidance.**	Yes	See Information Governance Handbook
1.2.2	**When were the data security and protection policy or policies last updated?**	17 October 2018	[not provided]
1.2.3	**Policy has been approved by the person with overall responsibility for data security.**	Yes	[not provided]
1.2.4	**Data Security and Protection Policies available to the public.**	https://bhdirectory.github.io/policy/ig-handbook.html	Link available to staff via their online training platform

1.2.5	**Staff awareness - Policies (Q2). I know the rules about who I share data with and how.**	[not provided]	[not provided]
1.2.6	**Staff awareness – Policies (Q3). I know who to ask questions about data security in my organisation.**	[not provided]	[not provided]
1.3.1	**ICO Registration Number.**	Z9046294	Tier 2
1.3.2	**Transparency information is published and available to the public.**	https://www.birtleyhouse.co.uk/privacy-policy/	[not provided]
1.3.3	**How have Individuals been informed about their rights and how to exercise them?**	https://www.birtleyhouse.co.uk/privacy-policy/protecting-your-personal-information-a-guide-for-Residents/	There are a couple of plain-English guides to our Data Protection policies available online. These have also been displayed in teh building and refereneced in our Quarterly Newsletter. https://www.birtleyhouse.co.uk/privacy-policy/protecting-your-personal-information-a-guide-for-Staff/

1.3.4	**There is a staff procedure about how to provide information about processing and individuals' rights at the correct time.**	https://bhdirectory.github.io/policy/ig-handbook.html#dp-dataRights	[not provided]
1.3.5	**There is an updated subject access process to meet shorter GDPR timescales.**	https://bhdirectory.github.io/policy/ig-handbook.html#subjectAccessRequests	[not provided]
1.3.6	**Provide details of how access to information requests have been complied with during the last twelve months.**	One SAR request received in the last 12 months. Request received by email on 12 November 2018. Responded to on 16 November 2018. Final response sent on 10 December 2018.	[not provided]
1.3.7	**Total ICO Fines in last 12 months.**	None	[not provided]
1.4.1	**A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing.**	Record of Processing Activities.xlsx	[not provided]
1.4.2	**Have information flows been approved by the person responsible for data security?**	Yes	As the SIRO I can confirm that the current identified information flows have been approved.
1.4.3	**Date of when information flows were approved by the person with responsibility for data security.**	04 March 2019	[not provided]
1.4.4	**Provide a list of all systems/information assets holding or sharing personal information.**	This list is available from the IG Lead and was reviewed March 13th 2019	[not provided]

1.4.5	**List of systems which do not support individual login with the risks outlined and what compensating measures are in place.**	All systems that contain personal information support individual login	[not provided]
1.5.1	**There is approved staff guidance on confidentiality and data protection issues.**	Yes	Within the IG Handbook is our Confidentiality Code of Conduct
1.5.2	**Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed.**	Yes	A set of discussion points around data protection is being introduced to regular Supervision sessions with staff
1.5.3	**Results of staff spot checks and actions taken when data protection non-compliance is identified.**	Supervision documents will contain evidence of staff member's responses to discussion topics	This will be rolled out over the next couple of months
1.5.4	**Staff awareness Question - Used legally and securely (Q4) …. I am happy data is used legally and securely in my organisation.**	[not provided]	[not provided]
1.6.1	**There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.**	Yes	[not provided]

1.6.2	**Data Protection by design procedure has been agreed.**	Yes	[not provided]
1.6.3	**There are technical controls that prevent information from being inappropriately copied or downloaded.**	All IT systems which involve the processing of personal information have technical controls	[not provided]
1.6.4	**There are physical controls that prevent unauthorised access to sites.**	Physical access controls are in place throughout the building to reflect risk	[not provided]
1.6.7	**There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.**	Yes	Following ICO guidance we have decided not to complete a DPIA due to the relatively small-scale of our processing activities, even those involving special category data and criminal records.
1.6.8	**The Data Protection Impact Assessment Procedure has been agreed by the person in the organisation with overall responsibility for data security.**	[not provided]	[not provided]
1.6.9	**The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessments is being carried out.**	[not provided]	[not provided]

1.6.10	**Have any unmitigated risks been identified through the Data Protection Impact Assessment process?**	[not provided]	[not provided]
1.6.11	**All high risk data processing has a Data Protection Impact Assessment carried out before processing commences.**	Yes	Not relevant due to small-scale
1.6.12	**All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.**	Yes	No unmitigated risks
1.6.13	**Data Protection Impact Assessments are published and available as part of the organisation's transparency materials.**	[not provided]	[not provided]
1.7.1	**There is policy and staff guidance on data quality.**	Yes	[not provided]
1.8.1	**There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.**	Yes	[not provided]
1.8.2	**A records retention schedule has been produced.**	Yes	[not provided]
1.8.3	**Provide details of when personal data disposal contracts were last reviewed/updated.**	new contract signed with SDR 23/03/2018 www.sdr-uk.com	[not provided]

2.1.1	**When was the last review of the list of all systems/information assets holding or sharing personal information?**	13 March 2019	[not provided]
2.1.2	**The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security.**	Yes	[not provided]
2.2.1	**Staff awareness - Shared securely (Q5) …. I know how to use and transmit data securely.**	[not provided]	[not provided]
2.2.2	**Staff awareness - Used legally and securely (Q6) …. I feel that confidentiality is more important than sharing information for care.**	[not provided]	[not provided]
2.2.3	**Staff awareness - Processes (Q7) …. The tools and processes used by my organisation make it easy to use and transmit data securely.**	[not provided]	[not provided]
2.2.4	**Staff awareness - Raising concern (Q8) …. I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination.**	[not provided]	[not provided]

2.3.1	**There is a data protection and security induction in place for all new entrants to the organisation.**	Yes	[not provided]
2.3.2	**All employment contracts contain data security requirements.**	Yes	The clause in existing contracts is supplemented by the need for all staff to read and acknowledge our Confidentiality Code of Conduct which directly links failures of data protection to disciplinary action. An exercise in getting all staff to sign the acknowledgement form is ongoing and will be completed by the end of March 2019.
2.3.3	**Staff awareness - Laws and principles (Q9) …. I understand the important laws and principles on data sharing, and when I should and should not share data.**	[not provided]	[not provided]

2.3.4	**Staff awareness - Data sharing questions (Q10) …. If I have a question about sharing data lawfully and securely I know where to seek help.**	[not provided]	[not provided]
2.3.5	**Staff awareness - Personal responsibility (Q11)…. I take personal responsibility for handling data securely.**	[not provided]	[not provided]
3.1.1	**A data security and protection training needs analysis has been completed.**	Yes	[not provided]
3.1.2	**Date of last data security and protection training needs analysis.**	05 March 2019	[not provided]
3.1.3	**Training Needs analysis has been approved by the person with overall responsibility for data security.**	Yes	[not provided]
3.2.1	**Staff awareness - Training (Q12) … The data security training offered by my organisation supports me in understanding how to use data lawfully and securely.**	[not provided]	[not provided]
3.3.1	**Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.**	96% completed the awareness course	We have used a Data Protection course provided by ELFY (https://elearningforyou.co.uk/)

3.3.2	**Average mark of first attempt of Level 1 Training.**	[not provided]	[not provided]
3.4.1	**Number of staff assessed as needing role specialist training.**	7 staff have been identified for additional training	[not provided]
3.4.2	**Number of staff completing advanced Data Security Training.**	1 staff member has been identified as needing to complete advanced training	[not provided]
3.4.3	**Details of any Other data security and protection specialist training undertaken .**	[not provided]	[not provided]
3.5.1	**SIRO and Caldicott Guardian have received appropriate Training.**	SIRO/IG Lead has undergone additional training in the form of two course made available through the OU's FutureLearn platform: Understanding the General Data Protection Regulation & Introduction to Cyber Security	[not provided]
4.1.1	**The organisation maintains a current record of staff and their roles.**	Yes	CoolCare HR Software
4.1.2	**For each system holding personal and confidential data, the organisation understands who has access to the information.**	IT Registered Users Log is a password protected excel workbook stored on the company server	[not provided]
4.2.1	**Date last audit of user accounts held.**	05 March 2019	[not provided]
4.2.2	**List of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.**	[not provided]	[not provided]

4.2.3	**Staff awareness - Access to information (Q13): The level of access I have to IT systems holding sensitive information, is appropriate.**	[not provided]	[not provided]
4.3.1	**All system administrators have signed an agreement which holds them accountable to the highest standards of use.**	Yes	An agreement for system administrators has been distributed for signature. These will be complet by the end of March 2019
4.3.2	**The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.**	[not provided]	[not provided]
4.3.3	**Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder.**	[not provided]	[not provided]
4.3.4	**List of all systems to which users and administrators have an account, plus the means of monitoring access.**	[not provided]	[not provided]

4.3.5	**Staff have provided explicit understanding that their activity of systems can be monitored.**	Yes	This is included as part of our Confidentiality Code of Conduct which all staff acknowledge that they have read.
5.1.1	**Dates of process reviews held to identify and manage problem processes which cause security breaches.**	No formal process reviews have taken place due to the fact that no breaches or near misses have yet taken place. A more formal system of review is being considered as prudent proactivity.	[not provided]
5.1.2	**List of actions arising from the process review, with names of actionees.**	[not provided]	[not provided]
5.2.1	**Scanned copy of the process review meeting registration sheet with attendee signatures and roles held.**	[not provided]	[not provided]
5.3.1	**Explain how the actions to address problem processes are being monitored and assurance given to the person with overall responsibility for data security.**	[not provided]	[not provided]
6.1.1	**A data security and protection breach reporting system is in place.**	Yes	IG Handook Data Security Policy, 2.5 Data Security Breach Procedures
6.1.2	**List routes available for staff to report data security and protection breaches and near misses.**	[not provided]	[not provided]

6.1.3	**List of all data security breach reports in the last twelve months with action plans.**	Yes	No incidents reported
6.1.4	**The person with overall responsibility for data security is notified of the action plan for all data security breaches.**	Yes	[not provided]
6.1.5	**Individuals affected by a breach are appropriately informed.**	Yes	No breaches
6.2.1	**Number of security and personal information breaches recorded.**	[not provided]	[not provided]
6.2.2	**Speed of data security and protection breach reporting.**	[not provided]	[not provided]
6.2.3	**Staff awareness - Reporting (Q14) - I know how to report a data security breach.**	[not provided]	[not provided]
6.2.4	**Number of breaches that have been reported to the Information Commissioner**	0	[not provided]
6.3.1	**Name of anti-virus product.**	Sophos Central Server Advanced and Sophos Central Endpoint Advanced	[not provided]
6.3.2	**Number of alerts recorded by the AV tool in the last three months.**	0	0 Web Threats; 1052 Policy Violations; 2 Policy Warnings Issued; 4 Policy Warnings Proceeded
6.3.3	**Name of spam email filtering product.**	[not provided]	[not provided]

6.3.4	**Number of spam emails blocked per month.**	4000	[not provided]
6.3.5	**Number of phishing emails reported by staff per month.**	[not provided]	[not provided]
6.4.1	**Number and details of incidents caused by a known vulnerability being exploited.**	[not provided]	[not provided]
6.4.2	**Have you had any repeat data security incidents of the same issue within the organisation.**	[not provided]	[not provided]
6.4.3	**Staff awareness - Incidents (Q 15) - When there is a data security incident my organisation works quickly to address it.**	[not provided]	[not provided]
6.4.4	**Staff awareness - Learning Lessons (Q16) - When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again.**	[not provided]	[not provided]
7.1.1	**There is an incident management and business continuity plan in place for data security and protection.**	Yes	[not provided]
7.1.2	**The incident plan has been approved by the person with overall responsibility for data security.**	[not provided]	[not provided]

7.1.3	**Staff awareness - Contingency plan (Q17) - If a data security incident was to prevent technology from working in my organisation, I know how to continue doing the critical parts of my job.**	[not provided]	[not provided]
7.2.1	**Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.**	[not provided]	[not provided]
7.2.3	**From the business continuity exercise which issues and actions were documented, with names of actionees listed against each item.**	[not provided]	[not provided]
7.2.4	**All emergency contacts are kept securely, in hardcopy and are up-to-date.**	Yes	[not provided]
7.2.5	**Location of hardcopy of emergency contacts.**	Essential Information Folder locatyed in the Nursing Office Emergency Response Team Folder located in the Central Admin Office	[not provided]
7.2.6	**Date emergency contact list updated.**	01 March 2019	[not provided]
7.2.7	**Date emergency contact list printed/shared.**	[not provided]	[not provided]
7.2.10	**Document any re-defined processes to respond to common forms of cyber attack in the last twelve months.**	[not provided]	[not provided]

8.1.1	**What software do you use?**	a spreadsheet of the latest versions of the software in use is held on our file server.	[not provided]
8.2.1	**List of unsupported software prioritised according to business risk, with remediation plan against each item.**	There is one identified piece of unsupported software which is scheduled for replacement over the next couple of months.	[not provided]
8.2.2	**Where it is not possible to upgrade/update software, reasons are given.**	[not provided]	[not provided]
8.2.3	**The person with overall responsibility for data security confirms that the risks of using unsupported systems are being treated or tolerated.**	Yes	[not provided]
8.3.1	**Provide your strategy for security updates.**	MS Server OS is controlled by Kaseya and is scheduled to be applied weekly on a Saturday. Sophos updates are applied automatically. VMware and Veeam are applied manually as required. Microsoft Windows and Office updates are the default automatic update. Similarly, with Sophos.	[not provided]
8.3.2	**How regularly do you apply security updates to desktop infrastructure.**	Microsoft Windows and Office updates are the default automatic update. Similarly, with Sophos.	[not provided]
8.3.3	**How often, in days, is automatic patching typically being pushed out to remote endpoints?**	[not provided]	[not provided]

8.3.4	**How many times, in the last twelve months has the person with overall responsibility for data security been notified where patches have not been applied for longer than two months, with reasons why?**	[not provided]	[not provided]
8.3.5	**List of where software updates have not been applied for longer than two months, with reasons why.**	[not provided]	[not provided]
9.1.1	**The person with overall responsibility for IT infrastructure confirms all networking components have had their default passwords changed.**	I can confirm that all default passwords are changed	[not provided]
9.1.2	**A Penetration test has been conducted in the last 12 months, which confirmed that all networking components have had their default passwords changed**	[not provided]	[not provided]
9.2.1	**A penetration test has been conducted in the last 12 months, which confirmed web applications were not vulnerable to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities.**	[not provided]	[not provided]

9.2.2	**The person with overall responsibility for IT has reviewed the results of latest penetration testing, with action plan against outstanding OWASP findings.**	[not provided]	[not provided]
9.3.1	**The annual IT penetration testing is scoped in negotiation between the business and the testing team, and uploaded.**	[not provided]	[not provided]
9.3.2	**The SIRO confirms the scope of the annual IT penetration testing is adequate, and that actions from the previous penetration testing are complete or ongoing (with reasons for non completion).**	[not provided]	[not provided]
9.4.1	**The person with overall responsibility for data security confirms the organisation has a data security improvement plan.**	[not provided]	[not provided]
9.4.2	**What are your top three data security and protection risks?**	[not provided]	[not provided]
9.4.3	**Evidence that your management team has discussed your top three data security and protection risks and what is being done about them?**	[not provided]	[not provided]
9.4.4	**Date for full implementation of the data security improvement plan.**	[not provided]	[not provided]

9.4.5	**Data security improvement plan status.**	[not provided]	[not provided]
10.1.1	**The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.**	A spreadsheet of information is held on the file server	[not provided]
10.1.2	**Contracts with all third parties that handle personal information are compliant with GDPR.**	[not provided]	[not provided]
10.2.1	**Basic due diligence has been undertaken against each supplier according to ICO guidance.**	Yes	Currently this is not done. A revised 'Approved Contractor Scheme' is being developed to include checks on IG standards.
10.2.4	**The person with overall responsibility for data security is assured that suppliers who are Data Processors are prepared for GDPR.**	[not provided]	[not provided]
10.3.1	**List of data security incidents – past or present – with current suppliers.**	[not provided]	[not provided]