THE BIS SERVICES LIMITED
Third Floor Offices at GHL House, 12-14 Albion Place, Maidstone, Kent, ME14 5DZ

Review Sheet

Last Reviewed	Last Amended	Next Planned Review
18 Jun '24	18 Jun '24	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 Data Security and Data Retention Policy and Procedure provides guidance and support on the measures and requirements in place at THE BIS SERVICES LIMITED. It has been reviewed with no significant changes. Section 4.6 has been updated to reflect statutory changes to retention periods and to clarify existing retention periods where an extra year has been added onto the statutory period. Underpinning Knowledge and Further Reading reference links have also been checked and updated.
Relevant legislation:	• Data Protection Act 2018 • UK GDPR
Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: GOV.UK, (2023), *Right to work checks: an employer's guide*. [Online] Available from: https://www.gov.uk/government/publications/right-to-work-checks-employers-guide [Accessed: 18/6/2024] • Author: NHS DIGITAL, (2021), *Records Management Code of Practice 2021*. [Online] Available from: https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf [Accessed: 18/6/2024] • Author: ICO, (2021), *UK GDPR guidance and resources*. [Online] Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ [Accessed: 9/12/2024] • Author: NHS Digital, (2023), *Data Security and Protection Toolkit*. [Online] Available from: https://www.dsptoolkit.nhs.uk/ [Accessed: 18/6/2024]
Suggested action:	• Encourage sharing the policy through the use of the QCS App • Share 'Key Facts' with all staff • Ensure relevant staff are aware of the content of the whole 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.

THE BIS SERVICES LIMITED
Third Floor Offices at GHL House, 12-14 Albion Place, Maidstone, Kent, ME14 5DZ

1. Purpose

1.1 To ensure that all THE BIS SERVICES LIMITED staff understand the principles set out in UK GDPR in relation to data retention and data security.
1.2 By reviewing this policy, THE BIS SERVICES LIMITED will be able to consider appropriate retention periods for the personal data it processes and ensure that it stores personal data for an appropriate period of time.
1.3 This policy will enable THE BIS SERVICES LIMITED staff to review the policies and procedures they have in place to ensure that personal data they process is kept secure and properly protected from unlawful or unauthorised processing and accidental loss, destruction or damage.
1.4 To support THE BIS SERVICES LIMITED 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

1.5 To meet the legal requirements of the regulated activities that THE BIS SERVICES LIMITED is registered to provide:

- Data Protection Act 2018
- UK GDPR

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following Clients may be affected by this policy:

- Clients

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 To enable THE BIS SERVICES LIMITED to ensure that its data retention and data security policies are UK GDPR compliant.
3.2 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

THE BIS SERVICES LIMITED
Third Floor Offices at GHL House, 12-14 Albion Place, Maidstone, Kent, ME14 5DZ

4. Policy

4.1 Data Retention

As a general principle, THE BIS SERVICES LIMITED will not keep (or otherwise process) any personal data for longer than is necessary. If THE BIS SERVICES LIMITED no longer requires the personal data once it has finished using it for the purposes for which it was obtained, it will delete the personal data unless it is required by law to retain the data for an additional period of time.

4.2 THE BIS SERVICES LIMITED may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by THE BIS SERVICES LIMITED that does not become apparent until a future date. THE BIS SERVICES LIMITED will consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by THE BIS SERVICES LIMITED will, for example, affect the likelihood of THE BIS SERVICES LIMITED needing to rely on records at a later date.
A link to the NHSX Records Management Code of Practice 2021 is available in the Underpinning Knowledge section. It is a guide in relation to the practice of managing records, with minimum retention periods for different types of records relating to health and care.

4.3 THE BIS SERVICES LIMITED may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by UK Visas and Immigration and Immigration Enforcement in respect of the retention of right to work documentation (see the "Underpinning Knowledge" section).

4.4 THE BIS SERVICES LIMITED understands that claims may be made under a contract for six years from the date of termination of the contract, and that claims may be made under a deed for a period of twelve years from the date of termination of the deed. THE BIS SERVICES LIMITED should therefore retain contracts and deeds as well as documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus six and twelve years respectively.

4.5 THE BIS SERVICES LIMITED will consider how long it needs to retain HR records. THE BIS SERVICES LIMITED should consider separating its HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specify different retention periods for each category of personal data. THE BIS SERVICES LIMITED recognises that determining separate retention periods for each element of personal data may be more likely to comply with UK GDPR.
THE BIS SERVICES LIMITED may decide, however, that separating its HR records into different elements is not practical, and that it can determine a sensible period of time for which to keep the HR records in their entirety.
The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that employee in the future. If, for example, THE BIS SERVICES LIMITED is concerned that an employee may suffer personal injury as a result of their employment, it may choose to retain its HR records for a significant period of time. If any such claim is unlikely, THE BIS SERVICES LIMITED may choose to retain its files for six or twelve years (depending on whether the arrangement entered into between THE BIS SERVICES LIMITED and the employee is a contract or a deed).

4.6 THE BIS SERVICES LIMITED will consider the following advice and guidelines when deciding how long to retain HR data for. THE BIS SERVICES LIMITED acknowledges that the suggested retention periods below are based on guidance within relevant legislation and, in some cases, reflect statutory requirements. THE BIS SERVICES LIMITED may choose to retain records for a longer period of time in case a dispute arises. For example, data that is potentially relevant to pay disputes may be retained for seven years after employment ends despite a shorter statutory retention period:

- Recruitment records - Six months after notifying candidates of the outcome of the recruitment exercise
- Immigration checks - Two years after the termination of employment. THE BIS SERVICES LIMITED may consider retaining for a further year to enable the fact of any dispute to reach the attention of THE BIS SERVICES LIMITED after the statutory two-year period has ended
- PAYE records - At least three years after the end of the tax year to which they relate
- Payroll and wage records for companies - Six years from the financial year-end in which payments were made
- Records in relation to hours worked and payments made to workers - Six years beginning with the day

on which the pay reference period immediately following that to which they relate ends

- Records required by the Working Time Regulations:
  - Working time opt out - Three years from the date on which they were entered into
  - Compliance records - Three years after the relevant period
  - Health assessment records for night workers - Three years after the relevant period
- Maternity records - Three years after the end of the tax year in which the maternity pay period ends. THE BIS SERVICES LIMITED may consider retaining for a further year to enable the fact of any dispute to reach the attention of THE BIS SERVICES LIMITED after the statutory three-year period has ended
- Accident records - At least three years from the date the report was made, or potentially longer if deemed appropriate given the possibility of ongoing relevance of the records. THE BIS SERVICES LIMITED may consider retaining for a further year to enable the fact of any dispute to reach the attention of THE BIS SERVICES LIMITED after the statutory three-year period has ended

4.7 THE BIS SERVICES LIMITED will consider for how long it is required to keep records relating to Clients. In doing so, THE BIS SERVICES LIMITED will consider the data retention guidelines provided by the NHS, if applicable. Those guidelines can be accessed by using the link in the "Underpinning Knowledge" section. If the NHS guidelines do not apply to THE BIS SERVICES LIMITED, THE BIS SERVICES LIMITED will determine an appropriate retention policy for Client personal data. THE BIS SERVICES LIMITED may choose to retain personal data for at least six years from the end of the provision of services to the Client, in case a claim arises in respect of the services provided.

4.8 Irrespective of the retention periods chosen by THE BIS SERVICES LIMITED, THE BIS SERVICES LIMITED will ensure that all personal data is kept secure and protected for the period in which it is held. This applies in particular to special categories of data.

4.9 THE BIS SERVICES LIMITED must record all decisions taken in respect of the retention of personal data. If the ICO investigates the policies and procedures at THE BIS SERVICES LIMITED, a written record of the logic and reasoning behind the retention periods adopted must be available.

4.10 THE BIS SERVICES LIMITED will implement processes for effectively and securely destroying and/or deleting personal data at the end of the relevant retention period. THE BIS SERVICES LIMITED will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. THE BIS SERVICES LIMITED will also consider circulating guidance internally to encourage staff to regularly delete their emails.

THE BIS SERVICES LIMITED will introduce policies relating to the destruction of hard copies of documents, including using confidential waste bins or shredding them.

4.11 Data Security

THE BIS SERVICES LIMITED will take steps to ensure that the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.12 THE BIS SERVICES LIMITED understands that all health and care organisations, as detailed below, are required to comply with the Data Security and Protection Toolkit. A link to an explanatory guidance note is included in the Underpinning Knowledge section. Compliance with the Data Security and Protection Toolkit facilitates compliance with UK GDPR.

THE BIS SERVICES LIMITED understands that all organisations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

4.13 THE BIS SERVICES LIMITED will implement and embed the use of policies and procedures to ensure that personal data is kept secure. The suggestions below apply in addition to the steps THE BIS SERVICES LIMITED is required to take pursuant to the Data Security and Protection Toolkit, if the toolkit applies to THE BIS SERVICES LIMITED.

THE BIS SERVICES LIMITED will bear in mind the following principles when deciding how to ensure that personal data is kept secure:

- Confidentiality - ensuring that personal data is accessible only on a need-to-know basis
- Integrity - ensuring that there are processes and controls in place to make sure personal data is accurate and complete
- Availability - ensuring that personal data is accessible when it is needed for business purposes of THE

BIS SERVICES LIMITED

- Resilience - ensuring that personal data is able to withstand and recover from threats

For paper documents, these will include, where possible:

- Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use
- Adopting a "clear desk" policy to ensure that personal data is not visible or easily retrieved
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Redacting personal data from documents where possible
- Ensuring that documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period
- Minimising the transfer of personal data from outside of business premises and, where such transfer cannot be avoided, ensuring that the paper documents continue to be kept confidential and secure

For electronic documents, the measures taken by THE BIS SERVICES LIMITED will include, where possible:

- Password protection or, where possible, encryption
- Adopting a 'clear screen' policy where users lock screens when they are away from their computers
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by THE BIS SERVICES LIMITED)
- The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by THE BIS SERVICES LIMITED)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipient

THE BIS SERVICES LIMITED will ensure that all business phones, computers, laptops and tablets are password protected.

THE BIS SERVICES LIMITED will encourage staff to avoid storing personal data on portable media such as USB devices. If the use of portable media cannot be avoided, THE BIS SERVICES LIMITED will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

4.14 THE BIS SERVICES LIMITED will implement guidance relating to the use of business phones and messaging apps. THE BIS SERVICES LIMITED understands that all personal data sent via business phones, computers, laptops and tablets may be captured by UK GDPR, depending on the content and context of the message. As a general rule, THE BIS SERVICES LIMITED will ensure that staff members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by UK GDPR and may need to be provided pursuant to a Subject Access Request (staff should refer to the Subject Access Requests Policy and Procedure at THE BIS SERVICES LIMITED for further details).

4.15 THE BIS SERVICES LIMITED will ensure that all staff are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. To achieve this, THE BIS SERVICES LIMITED will:

- Provide training to staff where necessary on security of personal data
- Consider, in particular, the likelihood that personal data (including special categories of data) will be removed from the premises of THE BIS SERVICES LIMITED and taken to, for example, Client's homes and residences
- Control access to premises
- Ensure that all staff understand the importance of maintaining the confidentiality of personal data away from the premises
- Take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access

4.16 THE BIS SERVICES LIMITED will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of UK GDPR. THE BIS SERVICES LIMITED understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as to CareCERT if it is required to comply with the Data Security and Protection Toolkit.
4.17 THE BIS SERVICES LIMITED will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.
4.18 Privacy by Design
THE BIS SERVICES LIMITED will take into account the UK GDPR requirements around privacy by design, particularly in terms of data security.
4.19 THE BIS SERVICES LIMITED understands that privacy by design is an approach set out in UK GDPR that promotes compliance with privacy and data protection from the beginning of a project. THE BIS SERVICES LIMITED will ensure that data protection and UK GDPR compliance is always at the forefront of the services it provides, and that it will not be treated as an afterthought.
4.20 THE BIS SERVICES LIMITED will comply with privacy by design requirements by, for example:

- Identifying potential data protection and security issues at an early stage in any project or process, and addressing those issues early on;
- Ensuring that the default position in projects involving personal data is privacy centres i.e. privacy by default; and
- Increasing awareness of privacy and data protection across THE BIS SERVICES LIMITED, including in terms of updated policies and procedures adopted by THE BIS SERVICES LIMITED

4.21 THE BIS SERVICES LIMITED will conduct Data Protection Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by THE BIS SERVICES LIMITED. A template Data Protection Impact Assessment along with the circumstances in which a Data Protection Impact Assessment should be conducted is available within the Data Protection Impact Assessment (DPIA) Policy and Procedure at THE BIS SERVICES LIMITED.

5. Procedure

5.1 THE BIS SERVICES LIMITED must consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect the processing activities at THE BIS SERVICES LIMITED). THE BIS SERVICES LIMITED appreciates that this is key for complying with the privacy by design requirements in UK GDPR.
5.2 THE BIS SERVICES LIMITED will review the periods for which it retains all the personal data that it processes.
5.3 THE BIS SERVICES LIMITED will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff. THE BIS SERVICES LIMITED will also consider providing training to staff in respect of data retention.
5.4 THE BIS SERVICES LIMITED will review the security measures currently in place in respect of all the personal data it processes.
5.5 THE BIS SERVICES LIMITED will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. THE BIS SERVICES LIMITED will keep a record of all policies and procedures it implements to demonstrate its compliance with UK GDPR.

6. Definitions

6.1 CareCERT

- The Care Computer Emergency Response Team, developed by NHS Digital. CareCERT offers advice and guidance to support health and social care organisations to respond to cyber security threats

6.2 Data Subject

- The individual to whom the personal data relates

6.3 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the UK General Data Protection Regulation

6.4 UK General Data Protection Regulation (UK GDPR)

- The UK GDPR is the retained EU law version of GDPR that forms part of English law

6.5 Personal Data

- Any information about a living person from which they are, or can be, identified (directly or indirectly) including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV, special categories of data (defined below) and opinions about or given by the individual

6.6 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data - at the point you collect it, you are processing it

6.7 Special Categories of Data

- Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Anybody who processes personal data on behalf of THE BIS SERVICES LIMITED should be made aware of and should comply with the policies at THE BIS SERVICES LIMITED in respect of data retention and data security
- Personal data will not be kept longer than necessary
- Personal data will be deleted when no longer needed
- Personal data may be held for longer than needed for the purposes of processing if there are justified reasons such as to meet regulations, insurance or other statutory requirements
- Retention periods are the decision of THE BIS SERVICES LIMITED, but guidance should be sought by referring to the Records Management Code of Practice 2021
- All personal data will be kept securely
- All retention periods need to be documented and justified
- THE BIS SERVICES LIMITED has effective and robust processes for destroying personal data
- THE BIS SERVICES LIMITED will comply with the Data Security and Protection Toolkit when necessary
- Electronic devices will be password protected to aid security
- Documents containing personal data are only shared with people who need to know the content

THE BIS SERVICES LIMITED
Third Floor Offices at GHL House, 12-14 Albion Place, Maidstone, Kent, ME14 5DZ

Key Facts - People affected by the service

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

- THE BIS SERVICES LIMITED will implement and embed the use of policies and procedures to ensure that all personal data processed about people affected by the services provided by THE BIS SERVICES LIMITED, including Clients, is retained and is kept secure and protected in accordance with UK GDPR

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:

ICO - Records Management and Security (Retention Schedule):
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/

Policies at THE BIS SERVICES LIMITED:

- Data Protection Impact Assessment (DPIA) Policy and Procedure
- Clear Desk Policy and Procedure
- Subject Access Requests Policy and Procedure

Outstanding Practice

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

- You have considered the personal data you process and adopted and documented appropriate retention periods for each type of personal data
- You have reviewed the security measures in place in respect of the personal data THE BIS SERVICES LIMITED processes
- You have reviewed and considered the documents and guidance referenced in the "Underpinning Knowledge" and "Further Reading" sections
- The wide understanding of the policy is enabled by proactive use of the QCS App

Forms

Currently there is no form attached to this policy.