# Data Security and Data Retention Policy

## Introduction

### Data Retention

As a general principle, Universel Ltd will not keep (or otherwise process) any personal data for longer than is necessary. If Universel Ltd 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.

Universel Ltd 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 Universel Ltd that does not become apparent until a future date. Universel Ltd should consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by Universel Ltd will, for example, affect the likelihood of Universel Ltd needing to rely on records at a later date.

Universel Ltd 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 the Home Office in respect of the retention of right to work documentation.

Universel Ltd understands that claims may be made under a contract for 6 years from the date of termination of the contract, and that claims may be made under a deed for a period of 12 years from the date of termination of the deed. Universel Ltd may therefore consider keeping contracts and deeds and documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus 6 and 12 years respectively

Universel Ltd will consider how long it needs to retain HR records. Universel Ltd may choose to separate 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. Universel Ltd recognises that determining separate retention periods for each element of personal data may be more likely to comply with GDPR.

Universel Ltd 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, Universel Ltd is concerned that an employee may suffer personal injury as a result of its employment with Universel Ltd, Universel Ltd may choose to retain its HR records for a significant period of time. If any such claim is unlikely, Universel Ltd may choose to retain its files for 6 or 12 years (depending on whether the arrangement entered into between Universel Ltd and the employee is a contract or a deed).

Universel Ltd will consider for how long it is required to keep records relating to Service Users. In doing so, Universel Ltd will consider the data retention guidelines provided by the NHS, if applicable.

If the NHS guidelines don't apply to Universel Ltd, Universel Ltd will determine an appropriate retention policy for Service User personal data. Universel Ltd may choose to retain personal data for at least 6 years from the end of the provision of services to the Service User, in case a claim arises in respect of the services provided.

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

Universel Ltd will record all decisions taken in respect of the retention of personal data. Universel Ltd recognises that if the ICO investigates Universel Ltd's policies and procedures, a written record of the logic and reasoning behind the retention periods adopted by Universel Ltd will assist Universel Ltd's position.

Universel Ltd will implement processes for effectively destroying and/or deleting personal data at the end of the relevant retention period. Universel Ltd 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. Universel Ltd will consider circulating guidance internally to encourage staff to regularly delete their emails.

Universel Ltd will introduce policies relating to the destruction of hard copies of documents, including by placing the documents in confidential waste bins or shredding them.

**Data Security**

Universel Ltd will take steps to ensure 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.

Universel Ltd 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 GDPR.

Universel Ltd understands that the following types of organisations must comply with the Data Security and Protection Toolkit:

- Organisations contracted to provide services under the NHS Standard Contract
- Clinical Commissioning Groups
- General Practices that are contracted to provide primary care essential services
- Local authorities and social care providers must take a proportionate response to the new toolkit:
    - Local authorities should comply with the toolkit where they provide adult social care or public health and other services that receive services and data from NHS Digital, or are involved in data sharing across health and care where they process confidential personal data of Service Users who access health and adult social care services
    - Social care providers who provide care through the NHS Standard Contract should comply with the toolkit. It is also recommended that social care providers who do not provide care through the NHS Standard Contract consider compliance with the toolkit as this will help to demonstrate compliance with the ten security standards and GDPR

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

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 documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period

For electronic documents, the measures taken by Universel Ltd will include, where possible:

- Password protection or, where possible, encryption
- Ensuring 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 Universel Ltd)
- 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 Universel Ltd)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipients

Universel Ltd will ensure that all business phones, computers, laptops and tablets are password protected.

Universel Ltd will encourage staff to avoid, storing personal data on portable media such as USB devices. If the use of portable media can't be avoided, Universel Ltd will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

Universel Ltd will implement guidance relating to the use of business phones and messaging apps. Universel Ltd understands that all personal data sent via business phones, computers, laptops and tablets may be captured by GDPR, depending on the content and context of the message. As a general rule, Universel Ltd 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 GDPR and may be provided pursuant to a Subject Access Request (staff should refer to the Universel Ltd Subject Access Policy and Procedure for further details).

Universel Ltd 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. Universel Ltd will provide training to staff if necessary. Universel Ltd will consider in particular, the likelihood that personal data, including special categories of data, will be removed from Universel Ltd's premises and taken to, for example, Service Users' homes and residences. Universel

Ltd will ensure that all staff understand the importance of maintaining the confidentiality of personal data away from Universel Ltd's premises and take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access to that personal data.

Universel Ltd will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of GDPR. Universel Ltd understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as to CareCERT if Universel Ltd is required to comply with the Data Security and Protection Toolkit.

Universel Ltd will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.

**Privacy By Design**
Universel Ltd will take into account the GDPR requirements around privacy by design, particularly in terms of data security.

Universel Ltd understands that privacy by design is an approach set out in GDPR that promotes compliance with privacy and data protection from the beginning of a project. Universel Ltd will ensure that data protection and GDPR compliance is always at the forefront of the services it provides, and that it won't be treated as an afterthought.

Universel Ltd 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; and
- Increasing awareness of privacy and data protection across Universel Ltd, including in terms of updated policies and procedures adopted by Universel Ltd

Universel Ltd will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by Universel Ltd. A template Privacy Impact Assessment is available within the Universel Ltd Initial Privacy Impact Assessment Policy and Procedure.

Universel Ltd will 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 Universel Ltd's processing activities). Universel Ltd appreciates that this is key for complying with the privacy by design requirements in GDPR.

Universel Ltd will review the periods for which it retains all the personal data that it processes.

Universel Ltd will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff. Universel Ltd will consider providing training to staff in respect of data retention.

Universel Ltd will review the security measures currently in place in respect of all the personal data it processes.
Universel Ltd will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. Universel Ltd will keep a record of all policies and procedures it implements to demonstrate its compliance with GDPR