



Chicks Records management policy

1 Introduction

- 1.1 Maintaining business records in a systematic and reliable manner is essential to comply with our legal and regulatory requirements, eg relating to data protection, tax and employment. It also reduces the costs and risks associated with retaining unnecessary information.
- 1.2 This record management policy has been developed to help staff properly manage the records of CHICKS. It sets out:
 - 1.2.1 what records are
 - 1.2.2 how records should be classified and stored
 - 1.2.3 how long different classes of record should be retained
 - 1.2.4 how records should be disposed of

2 Responsibility and application

- 2.1 The Data Protection Officer (DPO) is responsible for this policy.
- 2.2 This policy applies to all staff, which for these purposes includes employees, trainees, consultants and others as required.
All staff must be familiar with this policy and comply with its terms.

2.3 This policy does not form part of any employee's contract of employment and CHICKS may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3 **What are records?**

3.1 For the purposes of this policy, records are documents, communications and other materials that are written, recorded or otherwise machine readable. Records can exist in different formats including electronic, paper, book, facsimile, film, videotape, audiotape, and other formats available through existing and emerging technologies.

3.2 Voicemail, text or instant messages do not constitute records, except those that have been recorded and retained for business or regulatory purposes.

3.3 There are two types of records: business records and short-term records.

3.4 **Business records**

3.4.1 Business records are records created or received in the course of CHICKS's business that:

- (a) document a business-related event or activity
- (b) demonstrate a business transaction
- (c) identify individuals who participated in a business activity
- (d) support a business-related event, activity, or transaction, or
- (e) are needed for other legal, business, or compliance reasons

3.4.2 Business records must be properly classified, stored, retained and disposed of in accordance with this policy.

3.5 **Short-term records**

3.5.1 Short-term records are those with no enduring business or operational value, and which are not considered to be business records. These include:

- (a) general CHICKS-wide, division-wide or departmental announcements, notices or updates
- (b) unsolicited vendor bids and/or offers
- (c) unsolicited CVs
- (d) routine and general correspondence having only an immediate or short-term value, and
- (e) personal files, emails or other documents.

3.5.2 As a general rule, short-term records should be retained for no longer than 30 days. While they may be captured by routine backup processes, they should not be specifically stored at an off-site storage facility. On occasion, it may be necessary to retain short-term records for longer than 30 days if they are required for a business purpose. However, once the record is no longer needed, it should be destroyed promptly.

3.5.3 Short-term records, including any personal files, emails or other documents on CHICKS premises or systems, may become business records if they are relevant to a legal or business matter of CHICKS.

4 **Creation of records**

- 4.1 The individual or department that authored, created or is the primary custodian of a record is responsible for ensuring it is retained and destroyed in accordance with this policy.
- 4.2 All records and other communications pertaining to CHICKS's business are to be appropriately and accurately worded. You must act responsibly, lawfully and professionally when creating records regarding our business activities and/or on our systems.
- 4.3 CHICKS prohibits staff from creating records that are misleading, intentionally false, fraudulent, sexually explicit, abusive, offensive, harassing, discriminatory, profane, libellous, defamatory, unethical, or that violate any laws, regulations or internal policies.

5 **Classification and mark-up of business records**

- 5.1 Some business records require greater levels of protection than others. Business records must be appropriately classified and marked to ensure a level of protection commensurate with their confidentiality, sensitivity or importance to CHICKS.

5.2 **Classification of business records**

Business records are classified as:

- 5.2.1 restricted, and/or
- 5.2.2 confidential, or
- 5.2.3 general, or
- 5.2.4 public

- 5.3 It is not possible to list every possible type of record and say how it should be classified. Instead, you should consider the following questions and exercise your judgement.

Does the record include personal data?	See our data protection policy for a definition, but as a general guide this is data which identifies or can be used to identify an individual (the 'data subject'). Records that contain personal data must be classified as restricted and confidential.
Are we under an obligation to store, transmit, or delete the information in the record in a certain manner?	This obligation could be imposed by a regulator or a contractual agreement with a supplier or client.
What is the commercial or competitive value of this information?	Information that would be valuable to our competitors such as trade secrets, strategic plans, pricing information, or merger and acquisition activity must be classified as confidential.
What is the potential impact if the record is inadvertently disclosed, corrupted, lost or destroyed?	Classify records as either restricted or confidential if inadvertent disclosure or loss etc would have an adverse impact on: —an individual —our reputation, competitive position, revenue or —any of our customers, agents, suppliers or other partners
Is the record in the public domain?	Provided the record is in the public domain for legitimate reasons, eg not as a result of breach of confidence, the record should be classified as public.

See Appendix 1 for examples of how different records may be classified. If in doubt, consult the DPO

Mark-up of business records

Records classified as restricted or confidential must be marked as 'Restricted' and/or 'Confidential' in one or more of the following ways:

- 5.4.1 in the document header or footer
- 5.4.2 in the subject line of an email and/or the top or bottom of the body of the message
- 5.4.3 by way of a watermark in the Word, Adobe, PDF etc version of the document
- 5.4.4 by way of a stamp on the hard copy
- 5.4.5 on the digital file folder

5.5 In certain circumstances, it may be necessary to expand on the mark-up, eg:

- 5.5.1 'Restricted: do not forward, print or copy'
- 5.5.2 'Restricted: encryption required'
- 5.5.3 'Restricted: professional privilege'

5.6 The mark-up should be displayed on the front page and each subsequent page of the record.

6 **Retention of business records**

6.1 Business records must be retained as long as required by relevant laws and regulations and in accordance with CHICKS's business needs.

6.2 **Retention periods**

6.2.1 Our record retention schedule at Appendix 2 sets out how long records will normally be held and when the record will be destroyed. We periodically review and update the schedule with additional record types.

- 6.2.2 Business records should not be disposed of or destroyed before the relevant retention period expires.
- 6.2.3 Business records should not, however, be kept longer than the relevant retention period unless the retention period for that particular record has been suspended, as described at section 10 below.
- 6.2.4 Where more than one retention period applies to a record, it should be retained in accordance with the longest retention period, unless otherwise directed by the DPO.
- 6.2.5 If a record type is not listed in the record retention schedule and is not a short-term record (see 3.5 above), contact the DPO for guidance.

6.3 **Retention: drafts and duplicates**

- 6.3.1 Draft or duplicate copies of business records should be retained only while they are needed for valid business reasons and never longer than the applicable retention period in the record retention schedule. For more guidance, see our Version control and document management policy.

You should not send draft or duplicate records to an off-site storage facility without the approval of the DPO.

6.4 **Retention: format**

- 6.4.1 Most business records can be retained exclusively in electronic form and hard copies do not usually need to

- be retained.
- 6.4.2 Contracts and other legally binding records can be retained exclusively in electronic form, so long as the electronic record:
 - 6.4.2.1 accurately reflects the original, and
 - 6.4.2.2 is in a form that is capable of being retained and accurately reproduced for later reference throughout the required retention period
- 6.4.3 You should check with the DPO before retaining contracts or other binding records solely in electronic form.

7 Storage of records

- 7.1 All records covered by the Version control and document management policy must be managed and stored in accordance with its terms.
- 7.2 Business records must be stored on CHICKS's premises or at a secure location or website approved by CHICKS to provide physical or electronic storage facilities. See Appendix 1 for guidance on the level of security required for different classes of records.
- 7.3 The following records should not be retained at an off-site storage facility:
 - 7.3.1 short-term or other non-business records
 - 7.3.2 paper duplicates or convenience copies, or
 - 7.3.3 authoritative electronic records where no duplicates exist—these should be stored in the shared drive.

7.4 When archiving paper records at an approved storage facility, you must clearly label storage boxes as follows:

7.4.1 *Record Type*

7.4.3 Matter Type

7.4.4 Department

7.4.4 designated destruction date consistent with the Schedule

8 **Removal of business records**

You may remove business records from CHICKS's premises only for legitimate business purposes; you must return those records when no longer needed off-site for business purposes.

9 **Destruction of business records**

9.1 Business records must be destroyed at the end of the relevant retention period, unless the retention period has been suspended under section 10.

9.2 See Appendix 1 for guidance on the method of destruction required for different classes of business record.

9.3 As a general rule, short-term records should be retained for no longer than 30 days. While they may be captured by routine backup processes, they should not be specifically stored at an off-site storage facility. On occasion, it may be necessary to retain short-term records for longer than 30 days. However, once the record is no longer needed, it should be destroyed promptly.

9.4 Periodically, you should determine whether you have records in your control that should be discarded or destroyed pursuant to this policy.

9.5 If you have questions or concerns about retaining any records beyond the scheduled retention periods, you should contact the DPO before disposing of the records in question.

Suspending the destruction date

- 10.1 If a claim, audit, investigation, subpoena or litigation has been asserted or filed by or against CHICKS, or is reasonably foreseeable, we have an obligation to retain:
 - 10.1.1 all relevant records, including those that otherwise would be scheduled for destruction under the records retention schedule, and
 - 10.1.2 records that otherwise could have been disposed of as short-term records
- 10.2 On learning of an actual or reasonably anticipated legal action, the Chief Operations Officer (COO) will notify relevant staff to suspend disposal and destruction of applicable records. This is known as a 'litigation hold'.
- 10.3 If you become aware of an actual or anticipated claim, audit, investigation, subpoena or litigation, you must immediately report the matter to the COO and discontinue any scheduled disposal pending confirmation of whether litigation hold is required.
- 10.4 You must carefully and diligently comply with any litigation hold notices. In particular, you must not alter, dispose of, discard or destroy any records that are subject to litigation hold. You must also continue to retain any and all such records until the COO issues a notice indicating that the litigation hold has been lifted and that the retention and disposal of such records should resume in accordance with CHICKS's retention schedule.

Failure to comply

- 11.1 CHICKS takes compliance with this policy very seriously. Failure to comply puts both staff and CHICKS at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

11.2 Staff with any questions or concerns about anything in this policy should not hesitate to contact the DPO.

12 **Monitoring and review**

The DPO has overall responsibility for this policy. They will monitor compliance with this policy regularly to make sure it is being adhered to.

Appendix 1

Classification mark-up and storage examples

Record classification	Examples	How should the record be marked-up?	Security and destruction
Restricted	Personal and special categories of personal data, eg HR records. Records containing customer information that is regulated by law, eg credit card details.	<p>‘Restricted’ or, as required:</p> <p>‘Restricted: do not forward, print or copy’</p> <p>‘Restricted: encryption required’</p> <p>‘Restricted: do not forward, print, or copy’</p> <p>‘Restricted: named recipients only’</p> <p>NB: Records that contain personal data must be classified as ‘Restricted and confidential’.</p>	<p>Storage</p> <p>Secure in locked file cabinet, desk drawer or office.</p> <p>Do not leave unattended on monitor or desk when not in active use.</p> <p>Encryption or password protection required for storage on portable devices.</p> <p>Destruction</p> <p>Paper records should be shredded and digital records should be deleted from all sources.</p>
Confidential	Trade secrets and records containing non-	<p>‘Confidential’ or, as required:</p> <p>‘Confidential: do not forward, print or copy’</p>	<p>Storage</p> <p>Secure in locked file cabinet, desk drawer or office.</p>

Record classification	Examples	How should the record be marked-up?	Security and destruction
	<p>public and/or proprietary CHICKS information.</p> <p>Personal information that is not otherwise classified as restricted, ie does not constitute personal data, eg anonymised data</p>	<p>‘Confidential: encryption required’</p> <p>‘Confidential: do not forward, print, or copy’</p> <p>‘Confidential: named recipients only’</p>	<p>Do not leave unattended on monitor or desk when not in active use.</p> <p>Encryption or password protection required for storage on portable devices.</p> <p>Destruction</p> <p>Paper records should be shredded and digital records should be deleted from all sources.</p>
General business records	<p>Records containing non-confidential business information, eg</p> <ul style="list-style-type: none"> —product information —business processes —marketing materials —routine correspondence 	<p>No specific requirements but, as required, you should consider:</p> <p>‘Internal use only’</p> <p>‘Do not transfer outside CHICKS’</p>	<p>Storage</p> <p>No specific requirements.</p> <p>Destruction</p> <p>Place paper records in recycling bin.</p> <p>Delete electronic records and backup copies.</p>
Public	<p>Records containing publicly available information, unless that information contains data that is classified at a higher level (eg personal data).</p> <ul style="list-style-type: none"> —press release 	<p>No specific requirements</p>	<p>Storage</p> <p>No specific requirements.</p> <p>Destruction</p> <p>Place paper records in recycling bin.</p>

Record classification	Examples	How should the record be marked-up?	Security and destruction
	<p>—published accounts/financial results</p> <p>—public website pages</p> <p>—annual report</p> <p>Low Business Impact if disclosed.</p>		Delete electronic records and backup copies.