A CitNOW Company

Data Retention and Records Management Policy

Tootle

Last Updated: 13th November 2020

tootle.co.uk

9 Millars Brook, Molly Millars Lane, Wokingham, RG41 2AD

This data retention and records management policy (this "Policy") is intended to provide a framework to ensure CitNOW Video Ltd (t/as Tootle) a company registered in England and Wales with company number 09720206 whose registered office is at 9 Millars Brook, Molly Millars Lane, Wokingham, Berkshire, England, RG41 2AD (“Tootle”, "We", “Us”) retains records and information for an appropriate period in light of applicable legal regulatory and commercial requirements.

Records and data are critical Tootle assets that provide documentation of Tootle's organisation, business functions, policies, procedures, operations, decisions, and internal and external transactions. Failure to manage our records and data effectively may result in serious consequences, including interruption to our business, damage to our reputation, regulatory enforcement action, and adverse litigation effects.

This Policy applies to all Tootle entities and employees. It should be read in conjunction with other Tootle policies, including Tootle's:

- Privacy Policy: www.tootle.co.uk/privacypolicy
- [Internal] IT and Security Policy
- [Internal] Acceptable Use Policy
- [Internal] Server Security Policy
- [Internal] Information Classification Policy
- [Internal] Incident Management Procedure
- [Internal] Data Retention Schedule

The periods specified in this Policy will be regularly reviewed and updated to reflect changes in legislation or current commercial practices. Consequently, please ensure that you check this Policy for changes. The policy published on the website is the latest version, and is dated at the top.

Purpose of this Policy

The purpose of this Policy is to:

- satisfy regulatory and legal requirements
- enable records and data to be stored securely

- ensure records are disposed of at the right time, in a manner that protects their confidentiality
- enable records to be efficiently accessed and retrieved
- ensure effective management of documentation to manage litigation and investigations

Failure to comply with the procedures outlined in this document could result in:

- breach of regulatory and legal obligations leading to financial loss and reputational damage for Tootle
- record keeping not being secure and accessible
- records not being disposed of in a timely manner and/or their confidentiality being breached

1. Key Terms used in this Policy

In this Policy, a "record" is any document or other recorded or stored information—in whatever format or type—that supports, describes or records Tootle's activities, or is created or received in the course or conduct of Tootle's business.

Consequently, the definition of a record is very broad. It includes (by way of example) paper and electronic documents; forms; reports; manuals; correspondence; notes; memos; message slips; calendars; diaries; drafts; copies; paper files; electronically-stored information (including any information stored on a machine or device, computer files (such as spreadsheets, databases, word-processing documents, e-mail messages, multi-media files and presentations), electronic data compilations/databases, text messages, web contents, voice mail and other media, such as videotape, audiotape, or photographs.

However, a record does not extend to any document or communication that lacks any substantive relationship to Tootle or its business activities, for example junk e-mail, spam and personal items. These items are not subject to this Policy, and should be destroyed, unless they are subject to a Legal Hold (as set out in section 11 below).

The term "data" when used in this Policy includes any information or other data which is processed or stored by Tootle or on its behalf, in both hard copy and electronically.

Typically this data will be kept within or associated with a record. For clarity, this term also encompasses any meta-data relating to a record.

The term “data subject” (when used in this Policy) means a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

The term "personal data" (when used in this Policy) means any information (in whatever form) from which an individual person can be identified. If you have any questions about what is and is not personal data, please contact our DPO, dpo@citnow.com.

2. Responsibility for records and data management and retention

It is essential that Tootle complies with its regulatory and legal requirements in relation to retention of data, including the General Data Protection Regulation (the "GDPR"), any applicable limitation periods and any tax/financial requirements set by government bodies or regulators.

If you are a manager, you are responsible for ensuring this Policy is understood and applied by staff and contractors under your supervision. If your staff or contractors cease to be engaged by Tootle, you must assume responsibility for retaining their records in accordance with this Policy.

If you are senior management, you are responsible for ensuring that data is managed and retained in your function/department in accordance with this Policy. These responsibilities include:

- ensuring that this Policy is communicated to all staff and contractors within your function/department
- promptly communicating any "Legal Holds" (see section 11 below) to appropriate personnel in your function/department as necessary, ensuring that no records or data subject to Legal Hold obligations are disposed of while the Legal Hold is in force
- supervising proper disposal of records and data at regular intervals

- ensuring that any non-compliance is dealt with in a timely manner and in accordance with this Policy

Any questions concerning record retention should be directed to the DPO, dpo@citnow.com.

3. Creation of Records and Data

Tootle is committed to creating and maintaining complete, accurate, and trustworthy records and data in relation to all its business activities.

You are strictly prohibited from deliberately creating false or misleading records. You should appropriately and accurately word all records, and cause all records to reflect Tootle's ethical commitment.

Records should not contain any language that is misleading, fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, abusive, libellous or defamatory, or that violates any laws or regulations.

Records and data should not be used for improper purposes, or for any purposes other than Tootle's business purposes.

4. Creation of Records and Data – additional considerations for personal data

Where any records or data contain personal data, you should ensure that the collection and processing of that personal data complies with the Privacy Policy and Internal IT and Security Policy (where applicable).

In addition, you should ensure that a clear record is kept by Tootle of the following aspects:

- the identity of the Tootle group company or companies which is responsible for the collection and processing of that personal data
- the purposes for which that personal data is collected and processed
- a description of the categories of personal data and data subjects involved

- the categories of recipients to whom the personal data have been or will be disclosed
- details of transfers of personal data to a third country, including the identification of that third country and any safeguards in place to ensure that the personal data is afforded adequate protection in that country
- the envisaged time limits for erasure of the personal data (broken down by each different category of personal data, if appropriate), or at least any specific criteria to be used to determine those time limits
- a description of any specific technical and organisational security measures put in place to protect the personal data (i.e. beyond any measures which Tootle ordinarily has in place for protecting records and data)

5. Retain or delete data? Frequency of review

Each department should formally review whether records and data which it has processed or is in is possession should be archived or destroyed, and to ensure that this Policy is being complied with, at least annually.

A timetable should be drawn up setting out when and how records and data will be destroyed following the review. All internal approvals that need to be obtained to enable the completion of any data archiving or destruction activities (e.g. budget clearances, IT department sign off, etc.) must be obtained in sufficient time to allow relevant timescales to be met.

6. Application of data retention in respect of personal data

With regards to personal data (whether relating to customers (including individual sellers who use our website and services direct, and those sellers whose personal data is passed to us by our partners), individual contacts at dealers, employees (past and present), workers, suppliers and any other data subject) there is no fixed period for which we should retain such data—i.e. the relevant period will be determined by other factors, not the mere fact that particular data is 'personal data'.

It is important to balance any legal obligation we may have to retain records and data in certain circumstances, against any legal obligation to delete personal data once it is no

longer needed for the purposes for which it was collected. Further detail on specific retention periods is set out below.

7. Archiving practices

Records and data should be stored in a way that allows all those who could require access to it to be able to find and retrieve the records and data quickly.

Personal data should only be retained and accessed for as long as is necessary in accordance with the purposes for which we originally obtained that data (unless we have a lawful basis to retain such personal data or use it for additional purposes.

Personal data relates (which should be in accordance with our Privacy Policy or Internal Data Protection Policy) or for deletion in accordance with the retention periods in this policy.

If you consider that such personal data should be archived for public interest, scientific or historical research or statistical purposes, please contact the DPO, dpo@citnow.com.

Archiving records and data does not alleviate our obligation to retain records and data only for so long as is necessary for the purposes we originally collected it for. Where possible, all data that is to be archived should be marked with a destruction date. Archived data should be destroyed once the selected destruction date has passed.

Where records or data belonging to a third party is to be archived by Tootle, a central record of all records and data belonging to that third party, which is to be retained by Tootle should be kept. If the third party requests the return of its records or data, or your co-operation in dealing with requests from individuals in relation to those records or data, then Tootle needs to be able to identify where it can locate them.

8. E-mail retention

Wherever possible, and only where e-mails are not subject to specific retention periods, e-mails should not be retained beyond their immediate usefulness.

Personal e-mail folders should not be used to store business or other official records.

E-mails containing information which is likely to be required by Tootle staff other than the recipient of the e-mail should be stored to a central location where they can easily be accessed.

9. Giving third parties access to records and data

Any requests for access to or copies of records or data received from non-Tootle staff should be cleared through the DPO, dpo@citnow.com, before disclosure is made. Requests for personal data should be responded to in accordance with our Privacy Policy.

Where relevant, third parties should be asked to sign a standard non-disclosure agreement provided by Tootle before any information of a confidential nature is disclosed to them.

Any requests received from within Tootle or from external sources for disclosures of information to be made under the GDPR or other applicable data protection legislation, or from the police or other government departments, should be immediately passed to the DPO, dpo@citnow.com. For more information on such requests, please refer to our Privacy Policy or Internal IT and Security Policy as relevant.

When sending confidential or personal data, please ensure that appropriate encryption is used to protect the data in transition.

10. Engaging third party suppliers

All third parties who are engaged to prepare, process, hold, archive or delete records or data on our behalf should be asked to comply with specific data retention service levels, including (without limitation):

1. to comply with the provisions of this Policy
2. to only process the records and data we provide to them for purposes instructed to them by us
3. to keep Tootle's records and data with sufficient security to prevent the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to that data

These service levels should be agreed in writing. Please contact the DPO, dpo@citnow.com, in relation to engaging third party suppliers to prepare, process, hold, archive or delete records and data on our behalf.

11. Legal Holds

Whenever litigation, audit, governmental investigations or proceedings or internal investigations are pending or reasonably anticipated, it is important that a consistent approach is adopted to ensure that copies of records that may need to be used for such proceedings are kept, and that records are only disposed of in accordance with clearly defined policies.

If Tootle is involved in litigation, whether as claimant or defendant, it may need to rely on records, information and data as evidence to support its case. If these have been disposed of, or if incomplete information has been kept, the ability to bring a claim, or defend one, will be severely compromised.

Once legal proceedings have been commenced, it is generally necessary as a matter of law to disclose to the other side all information, both helpful and damaging, which relate to the dispute in question (this is known as "disclosure" or "discovery"). Such a disclosure process must always be managed by the DPO, dpo@citnow.com, and so any dispute or potential dispute should immediately be referred to them.

The obligation to disclose continues after litigation commences. Routine and one off destruction of documents, records and other relevant data and information should be stopped as soon as litigation is a possibility, until advised to the contrary by the DPO. If you are in any doubt as to whether you should destroy anything in these circumstances, please contact the DPO, dpo@citnow.com, immediately.

Selective destruction of data for the intention of concealing illegal activity or impeding an investigation is likely to be a criminal offence.

12. Data Destruction

When disposing of records or data, or any equipment upon which records or data have ever been stored, it is very important that measures are taken to ensure that all information (and in particular personal data and confidential data, whether of users, employees or suppliers) is irretrievably deleted.

All hardcopy confidential information (i.e. any document that is labelled "Confidential", "Proprietary Information" or "Trade/Business Secrets") and personal data that is to be destroyed should only be destroyed in a secure manner (preferably shredded). All other paper records may be placed in normal recycling bins.

If records or data are held on a computer (including any mobile electronic devices such as a smartphone) files, hard drives, memory sticks or other removable media, these records and data should be appropriately and irretrievably deleted or encrypted. Please note that simply deleting files from these sources using standard "delete" functions will not usually remove the file entirely.

13. Retention Periods

We have set out the periods for which we retain different categories of records and data in our internal Data Retention Schedule. Please review this carefully in order to ensure compliance with this Policy.

14. Failure to comply with this policy

The consequences to our business of failing to comply properly with our obligations relating to records management and data retention can be severe. As a result, failure to comply with this Policy shall be considered to be a disciplinary matter.