# Data Retention & Destruction Policy

## 1 INTRODUCTION & BACKGROUND

**Purpose**

In accordance with the principles of the Data Protection Act this policy covers all records and documents, regardless of physical form, containing guidelines for how long certain documents should be kept and how records should be destroyed.

**What does this Policy mean to me?**

The quantity and volumes of information (whether in electronic, hard copy print or hand written form) our business creates, receives and manages is growing at an exponential rate. Our Customers, Business Partners and People trust us to ensure we keep only the information that is reasonable and appropriate for us to run and operate our business. This policy makes sure that this trust is well placed.

We have defined our commitment, where practically possible, to not just manage our retention of documents but more importantly our commitment to the destruction of all documents and records that exceed our retention guidelines in a timely, consistent and uniform way.

This is a company-wide commitment. It is incumbent on each of us to ensure our compliance with this policy and to be vigilant in our destruction of the data that exceeds the agreed retention periods. Whilst, of course, not every schedule will apply to every area of Campbell & Kennedy Maintenance Ltd, you should familiarise yourself with the retention periods applicable to the documents and records that you deal with on a day-to-day basis.

Exceptionally, you may be alerted by the company's board of Directors (in the form of a "Stop Notice") that you are not to destroy documents which are, or may be, relevant to a legal dispute. If you are aware of a potential dispute, documents which may be relevant to that dispute should not be destroyed, but if you are in any doubt, speak to Gerry Kennedy (Managing Director).

The Policy applies to all Campbell & Kennedy Maintenance people and you are responsible for the information that you hold.

- If you are the Head of Department where information is stored, either on paper or electronically, then you must ensure that processes within your department adhere to this Policy.
- If you are the business owner or the system owner of any electronic system that involves the processing of information, then you must adhere to this Policy.
- If you are a person/business acting on behalf of Campbell & Kennedy, who has been afforded access to, or given extract(s) of, company data then you must also adhere to this Policy.

The Policy applies to information held in operational and production systems and in archive as well as that stored in system log files and in back-up. It also applies to all information held or processed by third parties on Campbell & Kennedy Maintenance Ltd's behalf, i.e. suppliers and data processors.

In keeping with ISO 9001 standards, random, regular and unannounced security checks can and will be undertaken by the IT Manager. All breaches found will lead to disciplinary action being taken against any offenders.

**Who to contact about this Policy?**

Any questions regarding this Policy should be directed to the Registered Data Controller for Campbell & Kennedy Maintenance Ltd and the Policy Manager Lynne Prior (l.prior@ckmaintenance.co.uk).

Impact of the Policy on Conditions of Employment/Contract of Engagement
This Policy does form part of your Contract of Employment/Contract of Engagement and can be enforced accordingly.

- **POLICY FOR INFORMATION RETENTION**

Campbell & Kennedy Maintenance Ltd shall retain information only for the specified retention periods set out in this Policy and shall then arrange for the prompt and secure disposal of that information.

Retention periods are set out in the retention schedule contained in Appendix C. In general, unless specifically required by legal or regulatory requirements, information must not be retained for more than six years from the date of creation and customer information for no more than seven years following the closure of a customer account.

Exceptions to this Policy must be approved by Gerry Kennedy (Managing Director).
All information must be disposed of in accordance with the company's security policies on document and data disposal.
Electronic data must be disposed of securely with no traceable elements remaining and be non-reversible.
Hardcopy information must be securely destroyed (using company-supplied shredders or confidential waste bins).

**Log Files**
Information held within log files created automatically during system operation shall be covered by this Policy. Entries shall be retained for the time required to meet the purpose of the log file, although information stored in the log files must not be kept beyond the retention periods stated in this Policy.

**Back-Up Data**
Back-up data is data kept solely for the purpose of replacing other data in the event of their being lost, destroyed or corrupted.

- Data stored in back-up must not be kept beyond the retention periods stated in this Policy.
- Payment Card Information subject to the PCI DSS Standard

We must not store or retain the following credit card information in any form subsequent to a credit card transaction being processed.

- Personal identification number (PIN) or the encrypted PIN block.
- Card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card, often referred to as CVV2, CV2, CSC or CVD) used to verify card-not-present transactions.
- Full contents of any track (full track, track, track 1, track 2, magnetic-stripe data) from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere).

One of the following for any system processing payment cardholder information will be implemented:

- A programmatic process (automatic or manual) to remove or sanitise the card holder data (to mask the Primary Account Number (PAN)), at least quarterly, stored cardholder data that exceeds requirements as defined in this retention policy; or
- A manual review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements as defined in this retention policy.

All cardholder data must be secured in the designated company data environments.

Credit card data must NEVER reside outside of the company data environments. If such data is discovered outside of these designated environments, you must report it to the company's 'Registered Data Controller' for investigation and arrangement for secure destruction.

**Currently Campbell & Kennedy Maintenance Ltd does not retain/store any credit/debit card data and no card/financial information is written down.**

**Stop Notices**

Exceptionally, data and documents must not be destroyed at the end of the retention period when:

- a Stop Notice has been issued for specified types of information (paper or otherwise); or
- circumstances exist that would justify a 'Stop Notice' being issued, i.e. there is current, pending or threatened litigation for which the information might be required as evidence or the business is the subject of any regulatory investigation to which the record may be relevant. The Managing Director or company Board Director will confirm if this is the case.

The Managing Director and/or Board Director will inform the business owners and system owners that a Stop Notice has been issued and those owners shall inform all appropriate users and resources with access to their systems to ensure compliance with the Stop Notice.

The business and system owner shall confirm compliance with the Stop Notice and will immediately inform the Managing Director (and company Registered Data Controller) of any non-compliance.

Once in place, and until the lifting of the Stop Notice, all information that is the subject of the Stop Notice should be retained in its existing form and must not be destroyed.

**Electronic Mail (E-Mail) and Instant Messaging**

Individuals are responsible for applying Data Retention Policy requirements to emails sent and received from their company email account and to instant messaging conversations (where applicable).
Emails and Instant Messages that contain no business information and are inconsequential (such as saying that you are running late for a meeting) are to be deleted promptly once they have been read and acted upon.

# IS & Data Security

**Data Control Principles**

**Campbell & Kennedy Maintenance Ltd** is wholly committed to adhering to the principles of the data protection act. This means that we not only value the information we manage and/or retain but we also ensure that access to such is limited to authorised users only. To this end we have implemented this data controls policy to ensure that we can provide adequate and effective protection of any information we manage. It is expected that all data users (**Campbell & Kennedy Maintenance Ltd** staff and other authorised individuals/entities) will not only work within these policy guidelines but will also operate within the spirit and ethics of protecting customer information from abuse and misuse.

The confidentiality, integrity and availability of Campbell & Kennedy's information and information systems are central to our success. This policy governs the acceptable use of the company's information and information systems and seeks to achieve an appropriate balance between information sharing and information protection.

This policy applies to all Campbell & Kennedy Maintenance system users accessing any Company and/or Sky data, which includes but is not limited to all employees (whether temporary, fixed term or permanent), contractors and sub- contractors. It applies equally to use or access from company premises or from a remote location via any connection.

**Policy Statement**

This policy applies to all system users ("System Users"), which includes but is not limited to all employees (whether temporary, fixed term or permanent), workers, contractors and subcontractors.
Any requests for exceptions or variations to this policy must be made in writing to the IS Security Manager.

The purpose of the Information Systems (IS) Security policy is to define safeguards to protect the confidentiality, integrity and availability of computerised information and systems (and their outputs) in use within the Campbell & Kennedy Maintenance Ltd group of companies and it applies throughout the group. These safeguards are to mitigate internal and external threats whether malicious or accidental.

Guiding Principles

The Company will promote best practices in all aspects of information systems security so that customer, system and all data (herein referred to as Company Data) is subject to the most appropriate level of protection.

Systems Users are individually responsible for ensuring that all Company data they process is managed in line with safeguards stated in this policy and are encouraged to maintain an active interest in all information security matters.

Information/data can only be received, extracted and/or forwarded via the acceptable and approved mediums of doing so (telephone (all calls are recorded (inbound and outbound)), company email, CRM, company letterhead hardcopy (including ISO accredited forms) and (incoming) general post (white mail)). All unauthorised mediums of data flow are not recognised, should not be used, and will be considered in breach of this policy and disciplinary actions will be progressed accordingly.

All suspected information system security breaches must be reported to Lynne Prior in the first instance.

Breaches of these policies may be regarded as misconduct and those responsible for such breaches may be subject to the Company disciplinary procedure.

This policy will be reviewed on an annual basis and maintained by IS Security and IT Management.

**Conditions and Rules**

**System Users**

All System Users must familiarise themselves with this policy upon joining the Company and ensure they keep up to date. System User access to any Company computer system must be by an approved unique set of login credentials. The Company reserves the right to revoke this access at any time.

***To ensure maximum password security all passwords will contain both alpha-numeric, with a mixture of upper and lower case, and 'symbol' characters. The minimum length of a password will be 6 characters with a maximum length of 12. Passwords will be changed every 6 months (maximum) and previous passwords cannot be reused.***

***All passwords will be created by the IS Team/Managing Director only and a central log of such will be retained by same. All passwords and IT accounts will be closed/erased upon employment/engagement termination by the IS Team/Managing Director within 48 hours of notification*.***

***All system activity, including password use, repeat password change requests etc., will be monitored and logged by the IS Team/Managing Director.***

***Passwords must not be written down nor shared with any other employee or person.***

**Campbell & Kennedy Maintenance HR Manager will notify the IT Team of any starters/leavers via emailing the respective starter/leaving form to g.kennedy@ckmaintenance.co.uk. Accounts will be created/terminated within 48 (working) hours of receipt.*

System Users must not attempt to access any Company systems or data that they have not been explicitly authorised to access.

System Users must only use Company approved and issued computer equipment and peripherals for processing Company data, this includes wireless enabled peripherals and removable/portable storage.

System Users are not permitted to install unlicensed software or software that has not been approved for operation on Company computer systems.

System Users must report any virus alerts or irregular/suspect system issues on their system to the IS Service Desk.

**Managers**

Managers are responsible for notifying the HR Business Manager to ensure system access is revoked in a timely fashion (e.g. Upon termination of employment (see above)).

Managers are responsible for advising System Users under their management to act in accordance with this policy.

Business Unit Managers (defined as managers with an operational accountability, as opposed delegated responsibility, for the running of a department) will risk assess Company data in terms of criticality and where necessary will consult with IS Security staff to apply the most appropriate protection level to safeguard the Company's and customers' interests.

Business Unit Managers must ensure that appropriate contractual arrangements, covering nondisclosure, data protection and legislative compliance, are agreed with third parties prior to exchanging, or allowing access to, Company data.

Business Unit Managers are responsible for ensuring that all data is stored only for as long as commercial operational requirements or regulations dictate and in accordance with Campbell & Kennedy's data retention and destruction policy.

**The Company**
The Company will implement appropriate controls under its obligations to comply with the following legislation/standards as may be amended or replaced from time to time:

- Data Protection Act (2018)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Sarbanes-Oxley Act (2002)
- Payment Card Industry Data Security Standard (2018)

The Company will promote awareness of security controls to System Users and their obligations under these legislation instruments/standards through timely circulars and updated information portals.

**Definitions of Data: -**

**Manual Data**
All hard copy information shall be used for its intended purposes only. Once the said information has achieved its intended purposes is shall be: -

a) Scanned and electronically attached to the relevant customer database record.
b) Or, scanned and appropriately named and stored within the relevant electronic documents folder.
c) And/or, securely shredded/destroyed.

Note: No hard copy data should be retained after use. Campbell & Kennedy Maintenance deploy e-storage principles and procedures which should be adhered to in all circumstances. All hard copy data should be placed within the confidential data receptacles after converting to an e-copy.

All received hard copy information shall be date stamped prior to processing.

All printed output should be collected immediately and not rendered, discarded or otherwise, viewable for any longer than is necessary.

All printed output should be controlled in keeping with the principles of this data policy and the data protection act (see note above).

All used/expired printed output/hard copy should be securely shredded/destroyed once its purpose has been achieved (see note above).

No staff member, or authorised individual/entity, shall be allowed to note down any customer information on any system other than those authorised/governed by **Campbell & Kennedy Maintenance Ltd.**

No customer information is to be taken out with the company premises without authorisation from your Line Manager/Company Director.

**Campbell & Kennedy Maintenance Ltd** employs a clear desk policy.

**Electronic Data**

Campbell & Kennedy Maintenance Ltd employ an IT support company to ensure all IT systems are protected from virus and unauthorised access. All system users have their own personal login credentials. All users will have varying levels of system access dependent on their individual authorisation privileges. Third party users are subject to extra security measures via remote access policies. All system access & use is subject to ongoing monitoring, review and access restrictions/removal should it be deemed appropriate in the interests of security.

The CRM which holds customer information has enabled an electronic footprint facility which logs who has access, created, made changes and/or deleted customer information/records. The CRM also restricts non-administration users to read/write access only. User logs are viewed periodically, or when operational needs require, to ascertain access/change history of customer records.

All access to PC, CRM and other systems are via user name/password with relative access level restricted privileges employed. The IS Team/Technical Director is responsible for monitoring and user access event review(s).

All users must adhere to the company policy on IT system 'acceptable use'.

All users should lock their workstation PCs/Laptops etc. when not working with or within the immediate vicinity of their computer system.

No removable storage devices/removable media are to be attached to any company computer system/PC/laptop without written authority from a Director/Managing Director.

No customer or personal information is to be emailed, or otherwise electronically transported, to an external 3rd party without the authorisation of your Line Manager/Company Director.

**PCI DSS (Payment Card Industry Data Security Standard)**

**Campbell & Kennedy Maintenance Ltd** is PCI certified and such certification is accredited annually via an approved security vendor (currently 'Trustwave') to ensure full data compliance. Hard copy of current certification will be placed within the company canteen area and electronic copy hosted within the policy section of the company intranet. The company Finance Manager is responsible for obtaining this annual certification and issues arising thereof. Technical support will be provided by the IS Team/Technical Director.

**External Storage Devices**

Use of any external storage device is forbidden unless authorised by a Campbell & Kennedy Maintenance company Director. All authorised devices must be inspected before and after use by the company IT Manager to ensure data integrity and appropriate cleansing. As a matter of procedure all end-of-use storage devices (including PC's) are data cleansed and will have their hard disk (or equivalent) physically destroyed and disposed of to ensure that the is zero risk of data leakage or breach(es).

**Web Data**

**Campbell & Kennedy Maintenance Ltd** employs a 'Privacy Policy' which governs electronic information display/transference which extends to all e-storage systems and all company owned websites.

**Campbell & Kennedy Maintenance Ltd (web) Privacy Policy is as follows:** -

*The site editor takes your right to privacy seriously, and wants you to feel comfortable using this web site. This privacy policy deals with personally-identifiable information (referred to as "data" below) that may be collected by this site. This policy does not apply to other entities that are not owned or controlled by the site editor, nor does it apply to persons that are not employees or agents of the site editor, or that are not under the site editor's control. Please take time to read this site's Terms of use.*

*1. Collection of data*

*Registration for an account on this site requires only a valid e-mail address and a user name that has not been chosen already. You are not required to provide any other information if you do not want to. Please be aware that the user name you choose, the e-mail address you provide and any other information you enter may render you personally identifiable, and may possibly be displayed on this web site intentionally (depending on choices you make during the registration process, or depending on the way in which the site is configured) or unintentionally (subsequent to a successful act of intrusion by a third party). As on many web sites, the site editor may also automatically receive general information that is contained in server log files, such as your IP address, and cookie information. Information about how advertising may be served on this site (if it is indeed the site editor's policy to display advertising) is set forth below.*

*2. Use of data*

*Data may be used to customize and improve your user experience on this site. Efforts will be made to prevent your data being made available to third parties unless (i) provided for otherwise in this Privacy Policy; (ii) your consent is obtained, such as when you choose to opt-in or opt-out for the sharing of data; (iii) a service provided on our site requires interaction with a third party, or is provided by a third party, such as an application service provider; (iv) pursuant to legal action or law enforcement; (v) it is found that your use of this site violates the site editor's policy, terms of service, or other usage guidelines, or if it is deemed reasonably necessary by the site editor to protect the site editor's legal rights and/or property; or (vi) this site is purchased by a third party, in which case that third party will be able to use the data in the same manner as set forth in this policy. In the event you choose to use links displayed on this web site to visit other web sites, you are advised to read the privacy policies published on those sites.*

*3. Cookies*

*Like many web sites, this web site sets and uses cookies to enhance your user experience — to remember your personal settings, for instance. Advertisements may display on this web site and, if so, may set and access cookies on your computer; such cookies are subject to the privacy policy of the parties providing the advertisement. However, the parties providing the advertising do not have access to this site's cookies. These parties usually use non-personally-identifiable or anonymous codes to obtain information about your visits to this site. You can visit the Network Advertising Initiative if you want to find out more information about this practice, and to learn about your options.*

*4. Minors*

*The site editor might not allow persons who are aged thirteen or younger to become members of this site. For more information, please contact the site administrator.*

*5. Editing or deleting your account information*

*You are provided with the ability to edit the information stored for your user account information during registration, by visiting your user account control panel. You can request that your user account be deleted; to do so, please contact the site administrator. Content or other data that you may have provided, and that is not stored within your user account, such as articles published, may continue to remain on the site at the site editor's discretion, even after your user account is deleted. Please see the site's Terms of use for more information.*

*6. Changes to this privacy policy*

*Changes may be made to this policy from time to time. You will be notified of substantial changes to this policy either by through the posting of a prominent announcement on the site, and/or by a mail message sent to the e-mail address you have provided, which is stored within your user settings.*

*7. No Guarantees*
*While this privacy policy states standards for maintenance of data, and while efforts will be made to meet the said standards, the site editor is not in a position to guarantee compliance with these standards. There may be factors beyond the site editor's control that may result in disclosure of data. Consequently, the site editor offers no warranties or representations as regards maintenance or non-disclosure of data.*
*8. Contact information: If you have any questions about this policy or about this web site, please feel free to contact the site administrator.*

**Data Passed to 3rd Parties**
All information passed to authorised 3rd parties must conform to this policy and have signed the data protection policy declaration.

**Human Resource Files**
All human resource information is securely stored within the HR files cabinets accessible only by the Human Resource manager and company Managing Director.

**Marketing**
Campbell & Kennedy Maintenance have adopted an 'opt out' principle for the purposes of sales and marketing development. Any customer who wishes to 'opt out' of marketing can do so verbally or in writing and this request will be carried out within 2 working days from original request. The **Campbell & Kennedy Maintenance '**Customer Records Management (CRM)' system contains an' opt out' facility.

**Reporting Breaches**
If you know or suspect anyone of not adhering to, or clearly breaching, this policy or the principles of the data protection act then please advise your immediate Line Manager AND the company's registered Data Controller (**Lynne Prior**) of this immediately. **Campbell & Kennedy Maintenance Ltd** record all reported breaches, potential or actual, in the data protection breach log. This log is securely stored by the company's registered Data Controller.

**GUIDELINES FOR INFORMATION RETENTION**

If you have data or a document that is not contained within the retention schedule in Appendix C, you should seek guidance from the company Registered Data Controller.

Information should be reviewed at regular intervals to determine which ones are to be retained or destroyed.

- Such intervals shall be at least quarterly.

In the case of the winding up/striking off of any part of the Campbell & Kennedy Maintenance group, certain records need to be retained, e.g. by virtue of the Insolvency Regulations 1994 or for other reasons (e.g. if the registers contain information not capable of being obtained from Companies House in the event that the company is restored to the register) – a review should be undertaken of applicable legislation at the time of winding up/striking off.

When you submit paper documentation to archive storage, you must set a date for destruction for that documentation, and it is your responsibility, not the archives' to ensure that compliance is demonstrated. Currently Campbell & Kennedy Maintenance do not employ an archived storage agreement and all hard copy information is, where applicable, stored on-site until securely destroyed.

## 4 EXEMPTION PROCESS

In exceptional circumstances, where any requirement or principle contained in this Policy cannot be met, an exception may be requested via the Managing Director. Provided that the exemption request is reasonable, proportionate and justifiable in the prevailing circumstances and does not expose Campbell & Kennedy Maintenance Ltd, its customers or employees to unacceptable risk.

**Appendix A Definitions and Abbreviations**

**Definitions used in this Policy**

"Closure of Customer Account" means the date at which the cancellation or termination of a Campbell & Kennedy Maintenance Ltd customer account takes effect.

"Personal Data" means data which relate to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of intentions of the data controller or any other person is respect of the individual.

"Payment Cardholder Information" means any of the following information from a payment card:

a) Sensitive Authentication Data,
b) the primary account number (PAN), if not masked, truncated, or securely hashed, or
c) the cardholder's name, payment card expiration date or service code when stored or used in conjunction with a PAN (as defined in (b)).

"PCI DSS" is the Payment Card Industry Data Security Standard, version 3.2.1 (May 2018), and superseding versions as in effect and applicable to Campbell & Kennedy Maintenance Ltd from time to time.

"Sensitive Authentication Data" is the security-related information from a payment card used to authenticate cardholders, such as (a) validation code or value used to verify "card-not-present" transactions, (b) contents of any track of the magnetic stripe, or (c) personal identification number (PIN), if appearing in plaintext or otherwise unprotected form.

Abbreviations used in this Policy

| | |
|---|---|
| CA 85 | Companies Act 1985 (as amended) |
| CA 06 | Companies Act 2006 |
| DPA | Data Protection Act 2018 |
| HSWA | Health and Safety at Work Act 1974 |
| IT(PAYE)R | Income Tax (Pay As You Earn) Regulations 2003 |
| MHSWR | Management of Health and Safety and Work Regulations 1999 |
| MLR | Money Laundering Regulations 2003 |
| OPS(SA)R | Occupational Pension Schemes (Scheme Administration) Regulations 1996 |
| RBS(IP)R | Retirement Benefits Schemes (Information Powers) Regulations 1995 |
| RIDDOR | Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 |
| SMP(G)R | Statutory Maternity Pay (General) Regulations 1986 |
| SSP(G)R | Statutory Sick Pay (General) Regulations 1982 |
| TMA | Taxes Management Act 1970 |
| WTR | Working Time Regulations 1998 |
| VATA | Value Added Tax Act 1994 |

**Appendix B Legislation and Regulation applicable to this Policy**

Companies Act 1985 (as amended)
Companies Act 2006
Data Protection Act 2018 (and Ireland's Data Protection Acts of 1988 and 2003)
Limitations Act 1980

## Appendix C RETENTION SCHEDULES

Information Retention

**Campbell & Kennedy Maintenance Ltd** follows the document/information retention procedures outlined below. Documents/Information that are (is) not listed, but are substantially similar to those listed in the schedule will be retained for the appropriate length of time in accordance with the operational validity of the data held.

**Corporate Records**

| | |
|---|---|
| Annual Reports to Companies House | Permanent |
| Articles of Incorporation | Permanent |
| Board Meeting and Board Committee Minutes | Permanent |
| Board Policies/Resolutions | Permanent |
| Bylaws | Permanent |
| Fixed Asset Records | Permanent |
| Inland revenue Information | Permanent |
| Contracts (after expiration) | 7 years |
| Correspondence (general) | 5 years |

**Accounting and Corporate Tax Records**

| | |
|---|---|
| Annual Audits and Financial Statements | Permanent |
| Depreciation Schedules | Permanent |
| General Ledgers | Permanent |
| Inland Revenue Tax Returns | Permanent |
| Business Expense Records | 7 years |
| Journal Entries | 7 years |
| Invoices | 7 years |
| Sales Records | 5 years |
| Credit Card Receipts | 3 years |

VAT records (any information relating to VAT), including:

- Orders
- Delivery notes
- Relevant business correspondence
- Appointment, sales and purchases and account books
- Sale and purchase invoices
- Self-Billing Agreements
- Credit or debit notes
- Records of daily takings
- Annual accounts
- Import and export documents
- Acquisitions and dispatches documents
- Bank statements
- VAT account — 6 years, or, if a relevant enquiry remains open, for at least as long as it remains open

*Where HMRC have given a ruling or there is an agreement in place on how to treat certain transactions including any option to tax these should be retained permanently*

**Bank Records**

| | |
|---|---|
| Bank Statements and Reconciliation | 7 years |
| Electronic Fund Transfer Documents | 7 years |

**Payroll and Employment Tax Records**

| | |
|---|---|
| Payroll Registers | Permanent |
| Earnings Records | 7 years |

PAYE records may be preserved 'in any form or by any means'. 'PAYE records' include;

- Wages sheets,
- Deductions working sheets,
- Forms P46,
- Forms P9 and P11D.
- All other PAYE documents
- Supporting documentation for completion of annual returns
- Details of Expense Payments
- Details of payments made to employees by a third party but arranged by Campbell & Kennedy.
- Supporting documentation for calculation of earnings and benefits paid to employees and Contributions on those earnings.

| | |
|---|---|
| For Contributions payable in respect of taxable benefits and expenses: | Not less than 4 years after the end of the relevant tax year. |
| Social Security (Contributions) Regulations, Sch 4, Para 26 | 6 years after the end of the tax year to which they relate. |
| Payroll Tax returns | 7 years |
| Other Inland Revenue Returns/Statements | 7 years |

**Employee Records**

| | |
|---|---|
| Employment and Termination Agreements | Permanent |
| Retirement and Pension Plan Documents | Permanent |
| Records Relating to Training, Promotion, Demotion or Discharge | 7 years after termination |
| Criminal Records Check Information | 5 Years (from last return*) |

**Previous CRB information is immediately (securely) destroyed upon receipt of updated data.*

| | |
|---|---|
| Accident Reports and Worker's Compensation Records | 5 years |
| Salary Schedules | 5 years |
| Employment Applications / CVs/Interview Notes etc. (non-engaged personnel) | 12 months* |
| Employment Applications / CVs (engaged personnel) | 24 months* |
| Codes of Conduct Policies | Permanent (Reviewed & updated regularly) |
| Self-Audit Checklists/Logs | 3 months |
| General Occupational Health Records | 7 years from employment termination* |

Control of Substances Hazardous to Health Regulations 2002 (COSHH)

| | |
|---|---|
| Health surveillance, including medical reports, of employees who are, or are liable to be, exposed to a substance hazardous to health | 40 years from date of last entry for each individual* |
| List of employees exposed to group 3 and 4 biological agents | 40 years* |
| Where any exposure may lead to a disease many years later (COSHH, Sch 9). | 40 years after last exposure* |

Ionising Radiation Regulations 1999 (IRR): Individual radiation dose assessments.

| | |
|---|---|
| | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made. |
| Reg. 21(3). | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made* |
| Radiation accident assessments for individuals | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made. |
| Reg 23(2). | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made* |
| Radiation health records | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made. |
| Reg. 24(3). | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made* |
| Overexposure report | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made. |
| Reg. 25(2). | Until person has attained the age of 75 but in any event for a minimum of 50 years after the records were made* |
| Control of Asbestos at Work: Regulations 2002 (CAWR) | |
| Health surveillance (including medical reports) | 40 years from date of last entry. |
| Reg. 21(1). | 40 years from date of last entry* |
| **Grant Applications and Contracts* | 5 years after completion |
| **Legal, Insurance and Safety Records** | Permanent |
| Copyright Registrations | Permanent |
| Insurance Policies | Permanent |
| Copyright Registrations | Permanent |
| Leases (see property records section (below)) | 15years after expiration |
| General Contracts /Agreements | 3 years after termination |
| Consents for the processing of personal and sensitive personal data | For as long as the data is held in respect of a living individual |
| Record of what fair processing notices/privacy policies were provided and when | For as long as the data is held in |

*Retained by HR Manager ONLY*

| | |
|---|---|
| | respect of a living individual |
| Subject Access Requests and responses | 12 months |
| Records relating to whistle-blowing | 7 years |
| Intelligence dissemination | 7 years |
| Law Enforcement Authorisation Records | 7 years |
| Requests for disclosure of personal information, either mandatory or elective upon Campbell &Kennedy | 24 months |
| Litigation Files | 6 years after settlement or final judgment (or expiry of any obligations or restrictions). |
| (If settled by settlement deed, retain for 12 years post conclusion). | |
| Complaint Files (Consumer and Regulator) | 6 years from closure of the complaint |
| Legal memoranda and opinions | 10 years |
| Records held on systems for fraud investigation (including customer account and payment details). | 6 years from first recording. |
| (Where fraud is indicated, 6 years after closure of an investigation). | |
| Health & Safety written statement | Permanent.<br>(If amended, previous version should be kept at least 6 years) |
| Record and minutes of consultations with safety representatives and committees | Permanently |
| Accident Book (Form BI510) required by Social Security (Claims and Payments) Regulations | 3 years from the date of each entry |
| Dish assembly and ladder test | Duration of employment + 7 years. |
| Working at Heights Certification | Duration of employment + 7 years. |
| H&S equipment check | Duration of employment + 7 years. |
| Certificate of electrical safety | 10 years |
| *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995* | |
| Report of any reportable injury, disease or dangerous occurrence | 3 years from date of entry for each reportable incident |
| RIDDOR Reg 7 | Permanently |
| *Management of Health and Safety at Work Regulations 1999* | |
| Significant findings of any risk assessment carried out to comply H&S and any group of employees identified by it as being especially at risk. | At least until a further assessment has taken place which renders the previous one obsolete. |
| Reg. 3(6) | Permanently. |
| *Regulatory Reform (Fire Safety) Order 2005* | |
| Fire risk assessment under reg. 9 of the Order – significant findings, measures to be taken and any group of persons identified as being especially at risk. | At least until a further |

| | |
|---|---|
| | assessment has taken place which renders the previous one obsolete. |
| *Noise at Work Regulations 1989 and Control of Noise at Work Regulations 2005 (including revisions thereof)* | |
| Noise exposure assessments | Until a further notice assessment is made or required. |
| *Factories Act 1961* | |
| General register and other records required to be kept under s. 140 of the Factories Act 1961. | 2 years from the date of last entry. |
| Factories Act, s. 141. | 2 years from the date of last entry. |

(The requirement to maintain a register and other records under s. 140 Factories Act 1961 was repealed on 6 April 2009 by SI 2009/605. Campbell & Kennedy Maintenance will retain any previously held register for 2 years from the date of the last entry in register before destroying).

| | |
|---|---|
| *The Hazardous Waste (England and Wales) Regulations 2005 SI 2005/894* | |
| Records of tipped (discharged) hazardous waste under Reg. 47. | 3 years after deposit of the waste (or, if waste permit held for site, until permit surrendered or revoked). |
| Reg. 47. | 3 years after deposit of the waste (or, if waste permit held for site, until permit surrendered or revoked). |
| Records of disposal or recovery of hazardous waste by other means under Reg. 48. | Where the hazardous waste is fully recovered, or remains at a transfer station (as the case may be) until it leaves the site and for 3 years thereafter (or, if waste permit held for site, until permit surrendered or revoked). |
| Reg. 48. | Where the hazardous waste is fully recovered, or remains at a transfer station (as the case may be) until it leaves the site and for 3 years thereafter (or, if waste permit held for site, until permit surrendered or revoked). |
| Producers', holders' and consignors' records under Reg. 49. | Whilst remain holder of waste and for at least 3 years after the date on which the waste is transferred to another person. |

| | |
|---|---|
| Reg. 49. | Whilst remain holder of waste and for at least 3 years after the date on which the waste is transferred to another person. |
| Carrier's records under Reg. 50. | At least 12 months from the date |

| | |
|---|---|
| | of delivery of the waste to its destination. |
| Reg. 50. | At least 12 months from the date of delivery of the waste to its destination. |
| Consignee's return to the producer, holder or consigner under Reg. 54. | 3 years. |
| *Control of Substances Hazardous to Health Regulations 2002 (COSHH)* | |
| Significant findings of risk assessment undertaken in accordance with reg 6 | At least until a further assessment has taken place which renders the previous one obsolete |
| Reg 6(4) | Permanently |
| Record of examination and maintenance of control equipment | 5 years |
| Reg 9 | 5 years |
| Record of exposure to hazardous substance at the workplace – general exposure | 5 years |
| Reg 10(5)(b). | 5 years |
| Record of exposure to hazardous substance at the workplace – personal exposure of identifiable employees | 40 years |
| Reg 10(5)(a). | 40 years |
| Record of specialist training for employees provided to comply with Reg. 12 | At least 6 years after employment ceases. |
| Accident and emergency plans required by Reg. 13 | 6 years after plan has been superseded or revised |

Campbell & Kennedy Maintenance should consider whether such records should be retained for a longer period given the potential value for defending civil actions.

| | |
|---|---|
| *Ionising Radiation Regulations 1999 (IRR)* | |
| Record of maintenance and examination of personal protective equipment | 2 years from date of examination |
| Reg. 10 | 2 years from date of examination |
| Record of reasons for implementing a system of dose limitation | 50 years |
| Reg. 11(2) and Sch 4, Pt II, para 17. | 50 years. |
| Record of specialist training for employees provided to comply with Reg. 14 | At least 6 years after employment ceases. |
| Radiation dosage measurements required by Reg. 18(3). | 2 years from date measurements recorded. |
| Reg. 18(5). | 2 years from date measurements recorded. |
| Record of maintenance and testing of measurement and control equipment | 2 years from date records were made. |
| Reg. 19(4). | 2 years from date records were made. |
| Summary of radiation dose assessments. | 2 years from end of calendar year to which the summary relates. |
| Reg. 21(7) | 2 years from end of calendar year to which the summary relates. |

| | |
|---|---|
| Report of investigation required by Reg. 22 | 2 years after date report was made. |

| | |
|---|---|
| Reg. 22(4). | 2 years after date report was made. |
| Record of testing of radioactive seals, etc. | 2 years after article is disposed of or until a further record is made following a subsequent test to that article. |
| Reg. 27(3). | 2 years after article is disposed of or until a further record is made following a subsequent test to that article. |
| Records of the quantity and location of radioactive substances | 2 years from the date on which they were made and, in addition, for at least 2 years from the date of disposal of that radioactive substance. |
| Reg. 28. | 2 years from the date on which they were made and, in addition, for at least 2 years from the date of disposal of that radioactive substance. |
| Reports of investigations carried out to comply with Regs. 30 and 32 | 50 years (or two years if minor incident). |
| Regs. 30(5) and 32(7). | 50 years (or two years if minor incident). |
| *Control of Asbestos at Work: Regulations 2002 (CAWR)* | |
| Significant findings of asbestos risk assessment under Reg. 6 | Duration of the work at the premises. |
| Reg. 6(4). | Duration of the work at the premises. |
| Plan of work required by Reg. 7 | Duration of the work at the premises. |
| Reg. 7(2). | Duration of the work at the premises. |
| Record of employee training, accident and emergency procedures | Permanently. |
| Records of maintenance and examination of control measures under Reg. 12 | 5 years. |
| Reg. 12(3). | 5 years. |
| Air monitoring records when health surveillance required. | 40 years. |
| Reg. 18(4). | 40 years. |
| Air monitoring records when health surveillance not required | 5 years. |
| Reg. 18(4). | 5 years. |

**Electronic Documents and Records**

| | |
|---|---|
| Electronic documents will be retained as if they were paper documents. | 5 Years from creation |
| Back-Ups of individuals file share and email | 5 Years |
| Call Recording Data | 12 months |
| Sales/Marketing/Product Literature | 5 Years from creation |
| Requests to be removed from marketing | Date of suppression + 6 months |

| | |
|---|---|
| Direct Marketing consents | As long as consent is active |

| | |
|---|---|
| Consumer records from 3rd parties | In accordance with relative licence period or 24 months (whichever is the sooner) |
| 'Warm Lead' Marketing | 24 months (unless request received to be removed from marketing then marketing removal element (noted above) becomes in force |
| Initiated customer information (.e. those who have said that they would like to receive Sky/Campbell & Kennedy Maintenance products/services but who do not proceed to order such goods/services (and in respect of whom an account will have been created on Campbell & Kennedy Maintenance systems) | 24 months (unless request received to be removed from marketing then marketing removal element (noted above)) |
| Customer account records ((including hard copy/electronic) | 6 years |
| Paper records including credit card data | Not held by the company |
| Paper records including direct debit/bank detail data | 12 months after account termination |
| Call recording data | 12 months |
| Other personal data records (including Records relating to the landlords of blocks of flats in which Sky is installed) | 6 years after completion of works |
| **Property Records (including Intellectual Property)** | |
| Deeds of title | Until sold or transferred |
| Leases (signed copies) | 15 years after expiry. |
| Subletting agreements (signed copies). | 12 years after expiry or termination. |
| CCTV footage | Minimum required to the extent that it contains images of identifiable individuals. As per DPA 1998. |
| Wayleave agreements | 12 years after expiry or termination. |
| Landlord's consents. | 15 years after surrender, expiry or termination of lease or memoranda of terms. |
| Licences. | 15 years after surrender, expiry or termination of lease. |
| Planning consents. | Until property sold or consent expires. |
| Listed building consents. | Until property sold. |
| Specifications (for new buildings and improvements). | Up to 25 years. |
| Bills of quantity. | Up to 25 years. |
| Agreements with contractors and consultants. | 15 years after project completed. |
| Surveys and inspections. | Permanently. |
| Architectural reports. | 25 years. |
| Structural engineering, mechanical and electrical engineering and drainage services reports. | |

| | |
|---|---|
| | 15 years. |
| Building condition surveys. | 25 years. |

| | |
|---|---|
| Asbestos inspections. | 40 years + |
| Conservation reports (historic and listed buildings). | 25 years. |
| Site surveys. | 25 years. |
| Maps, plans and drawings. | 25 years. |
| Maintenance contracts and related files. | 12 years after end of contract. |
| Maintenance schedules and programmes. | 15 years. |
| Maintenance log. | 15 years. |
| All documents relating to patents, trademarks, copyrights and any other intellectual property rights. | Permanently |
| Asset registers. | Permanently. |
| MOT certificates. | Until vehicle sold. |
| Vehicle registration documents. | Until vehicle sold. |
| Maintenance logs. | Until vehicle sold. |
| Sky Network Services: Network Architecture and Topology (including maps, plans, drawings) | 25 years from date of creation |
| C&K Network Services: Network Architecture and Topology – ducting | 5 years after obsolescence |
| C&K Network Services: meetings with suppliers (when minuted) – including negotiation notes (letters and emails) and clarifications | 6 years after performance |

## Appendix D Emergency Planning, Document Destruction & Compliance

Campbell & Kennedy Maintenance records will be stored in a safe, secure and accessible manner. Documents and financial files that are essential to keeping Campbell & Kennedy Maintenance operating in an emergency will be duplicated or backed up daily and maintained off site.

**Document Destruction**

Campbell & Kennedy's Managing Director is responsible for the ongoing process of identifying its records, which have met the required retention period and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by secure shredding.

Document destruction will be suspended immediately, upon any indication of an official investigation or when legal action is filed or appears imminent. Destruction will be reinstated upon conclusion of any investigation.

**Compliance**

Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against Campbell & Kennedy Maintenance Ltd and its employees and possible disciplinary action against responsible individuals. The Managing Director will periodically review these procedures with legal counsel or the organization's certified public accountant to ensure that they are in compliance with new or revised regulations.