

ELECTRICAL INDUSTRIES POLICY

RETENTION POLICY

1 ABOUT THIS POLICY

- 1.1 The corporate information, records, and data of The Electrical Industries Charity Limited, a company registered in England and Wales under number 02726030, whose registered office is at Rotherwick House, 3 Thomas More Street, London, England, E1W 1YZ (“**the Company**”) is important to how we conduct ourselves and manage employees.
- 1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our Company operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our Company.
- 1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.
- 1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.
- 1.5 This policy does not form part of any employee’s contract of employment, and we may amend it at any time.

2 SCOPE OF POLICY

- 2.1 This policy covers all data that we hold or have control over. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as “data”.
- 2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.
- 2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.
- 2.4 This policy applies to all units and functions of the Electrical Industry Charity.

3 GUIDING PRINCIPLES

Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4 ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all employees:** We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, Appendix B of this Policy, any communications suspending data disposal and any specific instructions from the Data Protection Champions. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 **The Data Protection Champions:** The Data Protection Champions are responsible for identifying the data that we must or should retain, and determining, in collaboration with the relevant teams, the proper period of retention. They also arrange for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate. They shall also be responsible for:

- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring, and updating in relation to this policy.

5 TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records:** Certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information:** Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Company and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data:** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.3 below for more information on this.

5.4 **Sensitive personal data:** Some personal data will constitute “special category” personal data under applicable data protection laws, which means using and holding this type of personal data represents a greater risk to us and to the individual if it is misused. This type of personal data should be handled with care and deleted promptly on expiry of the applicable retention periods.

5.5 **Confidential information belonging to others:** Any confidential information that an employee may have obtained from a source outside of the Company, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

6 RETENTION PERIODS

- 6.1 **Formal or official records:** Any data that is part of any of the categories listed in the Record Retention Schedule contained in Appendix B this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Data Protection Champions.
- 6.2 **Disposable information:** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of, should you require any guidance then please contact the Data Protection Champions.
- 6.3 **Personal data:** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. Please refer to our Data Protection Policy for further details.
- 6.4 **What to do if data is not listed in the Record Retention Schedule:** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Data Protection Champions.

7 STORAGE, BACK-UP AND DISPOSAL OF DATA

- 7.1 **Receipt of paper records:** We may still receive paper records from time to time which are received at our registered address. The Data Protection Champions will ensure these are scanned into the appropriate system and that the paper copy is destroyed appropriately after the process is complete.
- 7.2 **Storage:** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.
- 7.3 **Destruction:** Our Data Protection Champions are responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling.

- 7.4 The destruction of data must stop immediately upon notification from the Data Protection Champions that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the Data Protection Champions lift the requirement for preservation.

8 SPECIAL CIRCUMSTANCES

- 8.1 **Preservation of documents for contemplated litigation and other special situations:** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the Data Protection Champions inform you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Data Protection Champions determine those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

- 8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Data Protection Champions.

- 8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9 WHERE TO GO FOR ADVICE AND QUESTIONS

Questions about the policy: Any questions about retention periods relevant to your function should be raised with your function lead or the Data Protection Champions.

10 BREACH REPORTING AND AUDIT

- 10.1 **Reporting policy breaches:** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depends largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Data Protection Champions. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

- 10.2 No one will be subject to, and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 **Audits:** Our Data Protection Champions will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice) to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

11 **OTHER RELEVANT POLICIES**

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Data Protection Policy
- Safeguarding Policy
- Cyber Security Policy

APPENDIX A- DEFINITIONS

“Data” means all data that we hold or have control over and therefore to which this policy applies. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as “data”.

“Data Protection Champions” means our Data Protection Champions who are responsible for advising on and monitoring compliance with data protection laws, as named in our Data Protection Policy.

“Data Retention Policy” means this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

“Disposable information” means disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

“Formal or official record” means certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

“Non-personal data” means data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

“Personal data” means any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour.

“Record Retention Schedule” means the schedule attached to this policy which sets out retention periods for our formal or official records.

“Storage limitation principle” means data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the UK GDPR as the principle of storage limitation.

APPENDIX B - RECORD RETENTION SCHEDULE

The Electrical Industry Charity establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the Retention Policy.

1 Company records

Record	Retention period	Storage format	Reason
Certificate of incorporation https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Companyrecords/CertificateOfIncorporation1992.pdf	Indefinitely	Electronic	Companies Act 2006, s 15 (CA 2006)
New certificate of incorporation to reflect change of company name https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Companyrecords/CertificateOfIncorporationChangofNameEICdated07.01.2014.pdf	Indefinitely	Electronic	CA 2006, s 80
Memorandum & articles of association (signed original) https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Companyrecords/MemorandumandArticlesofAssociation23.07.1998.pdf	Indefinitely	Electronic	CA 2006, ss 8 and 18

Record	Retention period	Storage format	Reason
Accounting records	<p>3 years from the date on which the record was made (private companies)</p> <p>6 years from the date on which the record was made (public companies)</p>	Electronic	CA 2006, ss 386 and 388
<p>Records of all proceedings at directors' meetings, including:</p> <p>—board minutes;</p> <p>—minute books;</p> <p>—written resolutions of the board;</p> <p>—register of sealed documents.</p>	10 years from the date of the meeting	Electronic	CA 2006, s 248
Minutes of all proceedings of general meetings	10 years from the date of the meeting	Electronic	CA 2006, s 355

Record	Retention period	Storage format	Reason
Copies of all members' resolutions passed outside general meetings	10 years from the date of the resolution	Electronic	CA 2006, s 355
Register of directors and their residential addresses https://eeiba.sharepoint.com/CommonData/FINANCE/Trustees_and_Committee_Members/Trustee_List_21.07.2024.xlsx	Indefinitely for the register itself	Electronic	CA 2006, s 162
Directors' service contracts and any variations https://eeiba.sharepoint.com/CommonData/HR/008_Trustees/CONFIDENTIALITY_AGREEMENT_Andy_Roach.pdf https://eeiba.sharepoint.com/CommonData/HR/008_Trustees/CONFIDENTIALITY_AGREEMENT_Andy_Sturgess.pdf https://eeiba.sharepoint.com/CommonData/HR/008_Trustees/CONFIDENTIALITY_AGREEMENT_David_Pownall_signed_doc.docx https://eeiba.sharepoint.com/CommonData/HR/005_Staff_Information/Appointment_Trustee	7 years from termination or expiry of the contract, unless executed as a deed, in which case 13 years from termination or expiry	Electronic	Limitation Act 1980 ss 5, 8 CA 2006, ss 227 and 228

Record	Retention period	Storage format	Reason
<p>Register of secretaries</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Company_records/Appointment_of_Secretary_Jil_Nadolski.pdf</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Company_records/Appointment_of_Secretary_Michael_Parrish.pdf</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Company_records/Appointment_of_Secretary_Jessica_Vailima.pdf</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Retention_Policy/Company_records/Appointment_of_Secretary_Tessa_Ogle.pdf</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/RetentionPolicy/Company_records/Appointment_Secretary_Valerie_Austin.pdf</p>	<p>Indefinitely for the register itself</p>	<p>Electronic</p>	<p>CA 2006, s 275</p>
<p>Register of disclosed interests</p>	<p>Indefinitely for the register itself</p> <p>An old entry may be removed from the register if more than six years have elapsed since</p>	<p>Electronic</p>	<p>CA 2006, ss 793, 808, 816 and 817</p>

Record	Retention period	Storage format	Reason
	<p>the entry was made</p> <p>A third party may apply for an entry relating to them to be removed from the register, if it is incorrect</p>		

Employment/ Volunteer records

1.1 Personnel records

Record	Recommended retention period	Storage format	Reference
<p>Rejected job applicant records, including:</p> <p>—contact details;</p> <p>—application letters or forms;</p> <p>—CVs;</p>	<p>Six months after applicant is notified of rejection</p> <p>Application forms should give applicants the opportunity to object to their</p>	Electronic	<p>ICO Employment Practices Code para 1.7</p> <p>Equality Act 2010, s 123</p>

Record	Recommended retention period	Storage format	Reference
<ul style="list-style-type: none"> —references; —certificates of good conduct; —interview notes; —assessment and psychological test results. 	<p>details being retained</p>		
<p>Application records of successful candidates, including:</p> <ul style="list-style-type: none"> —https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff; —https://eeiba.sharepoint.com/CommonData/HR/HR and PD; —https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff; —https://eeiba.sharepoint.com/CommonData/HR/HR and PD; —application letters or forms; —copies of academic and other training received; —references; —correspondence concerning employment; 	<p>Seven years after employment ceases</p>	<p>Electronic</p>	<p>Limitation Act 1980, s 5 (LA 1980)</p>

Record	Recommended retention period	Storage format	Reference
<p>—CVs;</p> <p>—interview notes and evaluation forms;</p> <p>—assessment and psychological test papers and results.</p>			
<p>Criminal records information:</p> <p>https://eeiba-my.sharepoint.com/personal/desiree_edwards_electricalcharity_org/Documents/EICstaff/DBS_checks</p> <p>criminal records requirement assessments for a particular post</p> <p>criminal records information forms</p> <p>the Disclosure and Barring Service (DBS) check forms</p> <p>DBS certificates</p>	<p>Criminal records requirement assessments for a particular post—12 months after the assessment was last used</p> <p>All other information in this category—as soon as practicable after the check has been completed and the outcome recorded (i.e., whether satisfactory or not) unless, in exceptional circumstances, the manager of the</p>	<p>Electronic</p>	<p>DBS guidance for employers:</p> <p>Duration of criminal record check validity</p> <p>ICO Employment Practices Code Nov 2011, part 1.7.4</p>

Record	Recommended retention period	Storage format	Reference
	<p>applicable employee or volunteer assesses that it is clearly relevant to the ongoing employment relationship, e.g. to allow for consideration and resolution of any disputes or complaints, in which case, six months</p> <p>If the manager considers it necessary to keep the information for longer than six months, the DBS should be consulted</p>		
<p>Employment contracts, including: —https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff</p>	<p>Seven years after employment ceases, unless document executed</p>	<p>Electronic</p>	<p>LA 1980, ss 5, 8</p>

Record	Recommended retention period	Storage format	Reference
<p>—https://eeiba.sharepoint.com/CommonData/HR/HR and PD</p> <p>—personnel and training records</p> <p>—written particulars of employment</p> <p>—changes to terms and conditions</p>	as a deed, in which case 13 years after employment ceases		
<p>Directors' service contracts and any variations</p> <p>https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff</p> <p>https://eeiba.sharepoint.com/CommonData/HR/HR and PD</p>	Seven years from termination or expiry of the contract, unless executed as a deed, in which case 13 years from termination or expiry	Electronic	LA 1980, ss 5, 8 Companies Act 2006, ss 227, 228
<p>Copies of identification documents (eg passports)</p> <p>https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff</p>	Not less than two years from date of termination of employment	Electronic	Immigration (Restrictions on Employment) Order, SI 2007/3290, Art 6(1)(b)
<p>Identification documents of foreign nationals (including right to work)</p>	Two years and six months from date of	Electronic	Immigration (Restrictions on Employment)

Record	Recommended retention period	Storage format	Reference
https://eeiba.sharepoint.com/CommonData/HR/009_EIC staff	termination of employment		Order, SI 2007/3290, art 6(1)(b)
Records concerning a temporary worker	Seven years after employment ceases	Electronic	LA 1980, s 5
Employee performance and conduct records, including: —probationary period reviews; —review meeting and assessment interviews; —appraisals and evaluations; —promotions and demotions.	Seven years after employment ceases	Electronic	LA 1980, s 5
Records relating to and/or showing compliance with Working Time Regulations 1998 including: —registration of work and rest periods; —working time opt-out forms.	Two years from the date on which the record was made	Electronic	Working Time Regulations 1998, SI 1998/1833, reg 9
Redundancy records	Seven years from date of redundancy	Electronic	LA 1980, s 5

Record	Recommended retention period	Storage format	Reference
Annual leave records	Seven years after the end of each tax year	Electronic	LA 1980, s 5
Parental leave records https://eeiba.sharepoint.com/CommonData/HR/005_Staff Information	Seven years after the end of each tax year	Electronic	LA 1980, s 5
Sickness records	Seven years after the end of each tax year	Electronic	LA 1980, s 5
Records of return-to-work meetings following sickness, maternity etc	Seven years the end of each tax year	Electronic	LA 1980, s 5

1.2 Payroll and salary records

Record	Recommended retention period	Storage format	Reference
Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses https://eeiba.sharepoint.com/CommonData/FINANCE/Payroll	Seven years	Electronic	Taxes Management Act 1970, s 12B Finance Act 1998, Schedule 18, para 21

Record	Recommended retention period	Storage format	Reference
<p>Pay As You Earn (PAYE) records, including:</p> <ul style="list-style-type: none"> —wage sheets; —deductions working sheets; —calculations of the PAYE income of employees and relevant payments to them, the deduction of tax from, or accounting for tax in respect of, such payments; —all documents relating to any information which an employer is required to provide to HMRC under Form P11D (benefits in kind); — <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Payroll</p>	<p>Three years after the end of the tax year to which they relate</p>	<p>Electronic</p>	<p>Income Tax (Pay As You Earn) Regulations 2003, SI 2003/2682, reg 97</p>
<p>Records demonstrating compliance with national minimum wage requirements, including hours worked</p> <p>Payescape Payroll Platform and HREscape</p>	<p>Six years beginning with the day upon which the pay reference period immediately following that to which they relate ends</p>	<p>Electronic</p>	<p>National Minimum Wage Act 1998, s 9</p> <p>National Minimum Wage Regulations 2015, SI 2015/621, reg 59 (as amended by National Minimum Wage (Amendment) Regulations 2021, SI 2021/329)</p>

Record	Recommended retention period	Storage format	Reference
<p>Employee income tax and National Insurance returns and associated HMRC correspondence</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Payroll</p>	<p>Three years from end of tax year to which they relate</p>	<p>Electronic</p>	<p>Income Tax (Pay as You Earn) Regulations 2003, SI 2003/2682, reg 97</p>
<p>Statutory sick pay (SSP) records</p> <p>https://eeiba.sharepoint.com/CommonData/FINANCE/Payroll</p>	<p>Three years after the end of the tax year to which they relate</p>	<p>Electronic</p>	<p>The requirement to maintain SSP records for three years after the end of the tax year to which they relate was revoked in 2014, but an employer may still be required by HMRC to produce such records as are in his possession or power which contain, or may contain, information relevant to satisfy HMRC that statutory sick pay has been and is being paid.</p> <p>The Statutory Sick Pay (General) Regulations 1982, SI 1982/894, reg 13(A)</p>

Record	Recommended retention period	Storage format	Reference
<p>Wage or salary records (including overtime, bonuses and expenses) and payments to consultants and independent contractors</p> <p>On Xero platform</p>	Seven years	Electronic	Taxes Management Act 1970, s 43
<p>Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence</p> <p>https://eeiba.sharepoint.com/CommonData/HR/005_Staff/Information</p>	Three years after the end of the tax year in which the period of statutory pay ends	Electronic	Statutory Maternity Pay (General) Regulations 1986, SI 1986/1960, reg 26 (and other corresponding legislation)

2 Health and safety records

Record	Recommended retention period	Storage format	Reference
<p>Records of reportable injuries, diseases or dangerous occurrences</p> <p>—reportable incidents;</p> <p>—reportable diagnoses;</p> <p>—injury arising out of accident at work (including Electrical Industries Charity’s accident book).</p>	Three years from date of the entry	Electronic	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR 2013), SI 2013/1471, reg 12

Record	Recommended retention period	Storage format	Reference
On HREscape platform			
Lists or register of employees who have been exposed to asbestos dust, including health records of each employee	40 years from the date of the last entry made in the record	Electronic	Control of Asbestos Regulations 2012, SI 2012/63, reg 22(1)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry made in the record	Electronic	The Control of Lead at Work Regulations 2002 (CLAW 2002), SI 2002/2676, reg 10
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record	Electronic	The Control of Substances Hazardous to Health Regulations 2002 (COSHH 2002), SI 2002/2677, reg 11
Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH)	Where the record is representative of the personal exposures of identifiable employee— 40 years from the date of the last entry made in the record Otherwise, five years from the date of the last entry made in the record	Electronic	COSHH 2002, SI 2002/2677, reg 10(5)

Record	Recommended retention period	Storage format	Reference
Records of tests and examinations of control systems and protective equipment under COSHH	Five years from the date on which the record was made	Electronic	COSHH 2002, SI 2002/2677, reg 9
Medical records under the Ionising Radiations Regulations 1999	Until the person to whom the record relates reaches or would have reached 75 years of age, but in any event for at least 50 years from the date of last entry	Electronic	Ionising Radiations Regulations 1999, SI 1999/3232, reg 24

3 Health and safety records

Record	Retention period	Storage format	Reason
Records of reportable injuries, diseases or dangerous occurrences —reportable incidents; —reportable diagnoses;	3 years from date of the entry in the record	Electronic	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR 2013), SI 2013/1471, reg 12(2)

Record	Retention period	Storage format	Reason
—injury arising out of accident at work (including Electrical Industries Charity’s accident book).			
Health records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record	Electronic	The Control of Substances Hazardous to Health Regulations 2002 (COSHH 2002), SI 2002/2677, reg 11(3)
Records of monitoring of exposures to hazardous substances (where exposure monitoring is required under COSHH)	Where the record is representative of the personal exposures of identifiable employees— 40 years from the date of the last entry made in the record Otherwise, five years from the date of the last entry made in the record	Electronic	COSHH 2002, SI 2002/2677, reg 10(5)
Records of examinations and tests of engineering controls and respiratory protective equipment under COSHH	5 years from the date on which the record was made	Electronic	COSHH 2002, SI 2002/2677, reg 9(4)

4 Security records

Record	Retention period	Storage format	Reason
<p>IT security management</p> <p>Records which demonstrate IT systems used by the Electrical Industries Charity are safe and secure.</p> <p>Example: records demonstrating compliance regarding:</p> <ul style="list-style-type: none"> —pseudonymisation; —confidentiality; —restoration of data; —ongoing security testing; —risk assessments. 	<p>7 years from date of the record</p> <p>As a minimum, you must delete the personal data contained in the record.</p>	<p>Electronic</p>	<p>Evidential and business (predominantly information security)</p>
<p>IT security system update register</p> <p>Example: Records relating to:</p> <ul style="list-style-type: none"> —routine IT security and operational system updates; and 	<p>7 years from date of updated record</p> <p>As a minimum, you must delete the personal data contained in the register.</p>	<p>Electronic</p>	<p>Evidential and business (predominantly information security)</p>

Record	Retention period	Storage format	Reason
—updates to IT security systems/mechanisms following security incidents.			
IT application records Example: Records relating to the development, maintenance, oversight and security of different IT applications.	7 years from the date when the application is no longer in use or the supporting records are superseded As a minimum, you must delete the personal data contained in the record.	Electronic	Evidential and business (predominantly information security)

5 Marketing and business development records

Record	Retention period	Storage format	Reason
CRM (customer relationship management) records—of former, current and potential customers	5 years from last active engagement with customer	Electronic	Business
Direct marketing information relating to a current customer, ie a	5 years from last active engagement	Electronic	Business

Record	Retention period	Storage format	Reason
customer we have engaged with in the past 5 years			
Direct marketing information relating to a potential customer	5 years from data collection	Electronic	Business
Information recorded on marketing suppression lists, ie individuals who have notified as they do not wish to receive marketing communications	Individual entries on the suppression list must be deleted 50 years from the date the marketing opt-out request was received	Electronic	Evidential and business
Website cookie data for targeted advertising	12 months from the date the cookie or tracking code was created If records are retained after this date, all personal data must be removed	Electronic	Evidential and business
Lottery records including promotions, participants and winners https://eeiba-my.sharepoint.com/personal/desiree_edwards_electricalcharity_org/Documents/PowerLottery	7 years from the date of entry.	Electronic	Financial data/ business marketing

Record	Retention period	Storage format	Reason
https://eeiba.sharepoint.com/CommonData/FINANCE/004_Lottery			

6 Data protection records

Record	Recommended retention period	Storage format	Reason
<p>Registers</p> <p>Examples:</p> <ul style="list-style-type: none"> —data processing register or inventory; —register of processors; —information asset register. 	<p>Registers are maintained indefinitely</p> <p>Individual entries on each register should be deleted 7 years after the relevant processing ceased or any ongoing matters relating to the entry are closed, whichever is the later</p> <p>Superseded registers should be deleted after 7 years</p>	Electronic	Evidential and business
Management of data subject requests	3 years from the date the request is completed (including regulatory appeals, investigations and court	Electronic	Evidential and business

Record	Recommended retention period	Storage format	Reason
	<p>action), or last contact with data subject, whichever is later</p> <p>If records are retained after this date, all personal data must be removed</p>		
Data protection complaints	<p>7 years from end of relationship with customer (including any extension to the relation while dealing with the complaint)</p> <p>Where details of the complaint are retained beyond this period, eg for statistical purposes, all personal data must be removed</p>	Electronic	Evidential and business
<p>Data breach notification</p> <p>Example: Records demonstrating the notification of a data breach:</p> <ul style="list-style-type: none"> —internally; —externally, eg to the data subject or a regulator. 	<p>7 years from the date we became aware of the breach or regulatory/civil action is finalised, whichever is later.</p> <p>If records are retained after this date, all personal data must be removed</p>	Electronic	Evidential and business

Record	Recommended retention period	Storage format	Reason
<p>Correspondence and consultation with regulators</p> <p>Example: Requests for guidance, regulatory notifications, requests for approval and escalations to regulators (excluding formal investigations).</p>	<p>7 years from the date correspondence, consultations etc are concluded.</p> <p>If records are retained after this date, all personal data must be removed.</p>	<p>Electronic</p>	<p>Evidential and business</p>
<p>Compliance records</p> <p>Examples:</p> <ul style="list-style-type: none"> —records relating to compliance with regulatory requirements; —information asset or third party supplier assessments, data protection compliance audit documentation, external assessments etc; —processor compliance assessments and other records; —data protection impact assessments; —legitimate impact assessments; 	<p>7 years from the date the document is no longer active or has been superseded</p>	<p>Electronic</p>	<p>Evidential and business</p>

Record	Recommended retention period	Storage format	Reason
—international transfer impact assessments.			
Undertakings to regulators Example: Records of formal undertakings made to regulators.	7 years from the date the undertakings were given or discharged, whichever is later	Electronic	Evidential and business
DPO and privacy team, operational, oversight and assurance records	7 years from the date the document is no longer active or was superseded If records are retained after this date, all personal data must be removed	Electronic	Evidential and business

7 **Published or public records**

Record	Recommended retention period	Storage format	Reason
<p>Published news and updates</p> <p>Example: Dated newsletters, news press releases and articles relating to a specific, recent event.</p>	<p>5 years from date of first publication or (in the case of ongoing publication) the date the content ceased to be published</p>	<p>Electronic</p>	<p>Business and evidential</p>
<p>Other published materials</p> <p>Example: User manuals and public-facing policy documents.</p>	<p>10 years from date of first publication or (in the case of ongoing publication) the date the content ceased to be published</p> <p>As a minimum, you must delete the personal data contained in the record.</p>	<p>Electronic</p>	<p>Business and evidential</p>

8 Other non-public records

Record	Recommended retention period	Storage format	Reason
<p>Compliance and regulatory records</p> <p>Examples:</p> <ul style="list-style-type: none"> —risk register; —policy documents; —correspondence with regulators; —audits; —applications. 	<p>Registers are maintained indefinitely</p> <p>Individual entries on a register and other documents should be deleted 7 years after they cease to be relevant</p> <p>Superseded registers should be deleted after 7 years</p> <p>If records are retained after this date, all personal data must be removed</p>	<p>Electronic</p>	<p>Business and evidential</p>
<p>Documents with no formal retention requirement</p> <p>Examples:</p> <ul style="list-style-type: none"> —convenience copies; —unclassified records. 	<p>7 years from the date the record or document was created</p> <p>If records are retained after this date, all personal data must be removed</p>	<p>Electronic</p>	<p>Business and evidential</p>