



Data Protection Policy

Purpose

The purpose of this policy is to ensure that the staff, volunteers and trustees of Acorns 2 Oaks Ltd are clear about the purpose and principles of data protection and to provide clear guidelines and procedures, which are to be consistently followed.

Acorns 2 Oaks Ltd as a body is a Data Controller, and the Trustees are ultimately responsible for the policy's implementation, and accountable for non-compliance within the organisation.

Failure to adhere to the GDPR is unlawful and could result in legal action being taken against Acorns 2 Oaks Ltd or its staff, volunteers or trustees.

Contents

| | |
|----------------------------------------------------------------|---|
| Policy Statement | 2 |
| Data Protection Officer (DPO) | 2 |
| Principles..... | 3 |
| Procedures | 3 |
| Processing Access..... | 4 |
| Consent | 4 |
| Subject Access Requests | 4 |
| Accuracy | 4 |
| Storage | 5 |
| Retention & Disposal | 5 |
| Use of Photographs..... | 5 |
| Electronic Payment Information Security | 6 |
| Disclosure and Barring Service..... | 7 |
| Contracts with Data Processors | 7 |
| Compliance | 7 |
| Complaints | 7 |
| APPENDIX A – EYFS 2017 record keeping legal requirements | 8 |
| APPENDIX B – Data Retention Schedules | 9 |

Policy Statement

Acorns2Oaks Ltd (A2O) processes personal information about the individuals that access their services and Centres. This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper or electronically.

To safeguard against breaches in data protection, A2O adheres to the principles of the Data Protection Act 1998 and the General Data Protection Regulation (GDPR), which came into effect on 25th May 2018. A2O systems and procedures are designed to ensure data protection.

Acorns 2 Oaks Ltd regards the lawful and correct treatment of personal information as imperative to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals.

All staff, volunteers and trustees are made aware of the Data Protection Policy and the Confidentiality Policy.

| Terminology | |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data subject | Person whose personal data is being processed: children, parents, employees, trustees, volunteers, service users |
| Data controller | Acorns2Oaks and the employees |
| Data processor | External organisations or bodies that process data on behalf or with A2O (i.e. Bromley IT, Worldpay, Clarion, Quickbooks) |
| Personal data | any information relating to a person that can be used directly or indirectly to identify that person, e.g. name, photo, email address, bank details, posts on social networking sites, computer IP address |
| Sensitive personal data | information about racial or ethnic origin, political opinions, medical information and genetic and biometric data where it is used to uniquely identify an individual |
| Processing information or data | the act of: obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, dissemination, making it available, aligning, combining, blocking, erasing or destroying the data or information |

Data Protection Officer (DPO)

The GDPR also requires the appointment of a Data Protection Officer. The role of the DPO is to:

- monitor and update the organisation's processing policies, procedures and practices
- maintain the breach register
- liaise with the ICO regarding serious data breaches
- monitor and process Data Subject Access Requests
- undertake data audits and Privacy Impact Assessments (PIA), where needed
- obtain contracts for all data processors with whom A2O employs the services of

A2O's Data Protection Office (DPO) is: **Gaynor Murphy**

Principles

The GDPR regulates the processing of information relating to data subjects. This includes the obtaining, holding, using, disclosing, retention and disposal of such information, and covers computerised and paper-based data.

Acorns 2 Oaks adheres to the GDPR by complying with the following principles

Information must be:

- obtained fairly and legally
- recorded accurately
- stored safely
- used only for the intended purpose
- disposed of securely when it is no longer appropriate to keep it
- not transferred to countries outside of the EU

Information must also be processed in accordance with the data subject's rights to:

- have access to their personal data held by the organisation, within 1 month of initial request
- have inaccuracies corrected
- have information erased
- prevent direct marketing
- prevent automated decision-making and profiling
- have data portability

Data Protection means that Acorns 2 Oaks must:

- manage and process personal data properly
- protect individual's rights to privacy
- provide an individual with access to all personal information held on them
- obtain complicit consent for the retention of data and communicate the organisation's Privacy Notice
- have contracts in place with verified external data processors, who are compliant in storing and processing data within the EU only

Data should be:

- protected by strong passwords that are changed regularly and never shared
- not be shared informally
- not be left open on screens of computers or in places available to the public

Procedures

Acorns 2 Oaks Ltd obtains both personal and sensitive personal data from staff, volunteers and trustees, children, parents, services users and service providers. The following procedures are in place to ensure that Acorns 2 Oaks Ltd is compliant with the processing of this data. Data is stored and processed for the following purposes:

- to assist in the efficient, safe and compliant provision of services
- for the purposes outlined in service agreements and specification
- recruitment and Staff Development
- equal Opportunities monitoring
- funding Opportunities
- volunteering Opportunities
- payroll
- to distribute relevant organisational material e.g. meeting papers

Processing Access

1. Access is limited to the organisation's staff, volunteers and trustees, and only to data permitted by their job role.
2. Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies, such as HMRC, Local Authority, Ofsted and/or as dictated by law or legislation, such as safeguarding or health & safety.
3. A copy of emergency contact details will be kept in the Emergency File for Health and Safety purposes.
4. PC's are password protected with timing out systems in place to deter electronic stored data being left open.
5. Confidential shredding is carried out either immediately or stored short term in a locked cabinet in the Executive Office.

Consent

1. When data is initially collected, the data subject will be given a copy of the respective Privacy Notice requesting their agreement.
2. The Privacy Notices are legal documents that advise the data subject of our commitment and approach to data protection.
3. Completed Privacy Notices are stored securely along with the data subject's information, for the defined retention period.
4. Consent is required in all circumstances, except in the case of childcare settings as these are bound by the legal requirement of the Early Years Foundation Stage (EYFS) 2017 to maintain records, obtain and share information with Parents and other professionals working with the child. The EYFS clauses pertaining to this requirement is detailed as an appendix in this policy.
5. Data will not be passed on to anyone outside the organisation without explicit consent from the data subject unless there is a legal duty of disclosure under other legislation, in which case the Chief Executive will discuss and agree disclosure with the Chair/ Vice Chair.

Subject Access Requests

1. Individuals have the right to access their data and supplementary information.
2. The right of access allows individuals to be aware of and verify the lawfulness of the processing.
3. Individuals will have the right to obtain confirmation that their data is being processed, access to their data and supplementary information corresponding to the information provided in the privacy notice (retention schedule etc)
4. All Access Requests are to be forwarded immediately to the DPO, who will log the request and oversee the process.
5. Information will be provided without delay and at the latest within one month of receipt.
6. The DPO may be able to extend the period of compliance by a further two months where requests are complex or numerous, informing the individual within one month of the receipt of the request and with explanation as to the need of an extension.

Accuracy

1. A2O will take reasonable steps to keep data up to date and accurate.
2. Any amendments provided by Data Subjects will be actioned without delay.
3. Where Clarion texts fail delivery due to incorrect number, the number will be removed from the Clarion system and the recipient contacted by other means as to obtain correct details.

Storage

1. Data is kept in paper-based systems, password-protected cloud-based computer system and password-protected accountancy software.
2. USB Sticks are **not to be used**.
3. Every effort is made to ensure that paper-based data is stored in organised and secure systems.
4. Electronic data will be protected by password and firewall systems
5. Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data

Retention & Disposal

Data will be retained only as long as it is legitimately required and disposed of safely and confidentiality.

The Data Retention Schedule in *Appendix C*, is compiled in accordance with the Pre-School Learning Alliance and the National Day Nurseries Association, and sets out:

1. the requirements and recommendations for retaining different types of records and information
2. the retention periods for each specific record type
3. how and when the data is archived
4. how and when the data is disposed

Wherever possible, archived data is scanned and stored electronically, and password protected on Office 365.

1. Only senior management and key personnel have access to these files.
2. Data files are organised in folders respective of the data source Personnel, Nursery etc.
3. Scanned data must be as eligible as the paper based original.
4. Once scanned, paper originals must be destroyed without delay by either in-house cross shredding or bulk confidential shredding by an external verified provider. In the interim, the paper originals must be stored securely.
5. Electronic data is destroyed by deletion from the system, ensuring the electronic recycling bin are emptied immediately thereafter.
6. Archiving and data disposal will take place periodically during the year.
7. Data files containing personal or sensitive data are labelled:
 - (a) Nursery: data subject initials and leaving year + 3 or 24 years (Mary Smith left 2017 = MS20)
 - (b) Employee: initials and short date of birth (Richard Taylor 15th June 1970 = RT150670)
 - (c) Youth Club: initials and short date of birth (John Wright 18th Feb 2005 = JW180205)

Use of Photographs

A2O will obtain consent from individuals before taking and displaying photographs in which they appear. Such displays can be in or around the Centre's or on the website. Group photos must only include individuals whom have given consent. If any doubt exists as to consent, the photograph must not be taken.

Photographs are to be displayed or uploaded as soon as possible and should be deleted from the cameras memory card or tablet immediately thereafter. Printed photos should be destroyed via cross shredding. Photographs play a key role in observing and demonstrating children's learning development. Upon leaving the setting, the child's learning journal, which contains most photographs taken, will be passed to the next setting or the child's parent/carer. Any photographs on display at the Nursery will be disposed of.

Electronic Payment Information Security

A2O processes sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations.

A2O commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. A2O are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should ensure:

1. company and cardholder information are handled in a secure manner
2. passwords and accounts are secure
3. all necessary steps are taken to prevent un-authorized access to confidential data which includes card holder data, i.e. always leave desks clear of sensitive cardholder data and lock computer screens when unattended
4. all sensitive cardholder data must be protected securely if it is to be transported physically and card holder data must never be sent over the internet via email, instant chat or any other end user technologies
5. new software, hardware, third party connections, etc. are only installed by the authorised IT Administrator and only after approval from the Chief Executive and the DPO
6. sensitive card data that is no longer required by A2O for business reasons is discarded in a secure and irrecoverable manner
7. information security incidents must be reported, without delay, to the DPO

It is strictly prohibited to store:

1. the contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. the CVV/CVC (the 3 or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. the PIN or the encrypted PIN Block under any circumstance.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert your line manager and the DPO immediately, who will carry out an initial investigation of the suspected security breach.
2. Upon confirmation that a security breach has occurred, the DPO will advise the data subject, record the details of the breach in the register and inform the ICO if applicable.

If the data security compromise involves credit card account numbers, implement the following procedure:

1. Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
2. Inform the DPO immediately.
3. Alert all affected parties and authorities such as the Bank, the credit card Fraud Control, and the police.
4. Provide details of all compromised or potentially compromised card numbers to Fraud Control.

Disclosure and Barring Service

Acorns 2 Oaks Ltd will act in accordance with the DBS's code of practice and as detailed on the Data Retention Schedule. From April 2019, electronically stored copies of current disclosures will be kept for the duration of an individual's employment or involvement with A2O and the following basic information is stored on a secure database, accessed only by the Executive Team. These procedures are in-line with LADO's Safeguarding Principles.

- date of issue
- name of the subject
- type of disclosure
- position for which the disclosure was requested
- unique reference number and the details of the recruitment decision taken.

Contracts with Data Processors

A2O employs the services of external processors, such as IT support companies, communication companies and accounting software. All these data processors have been verified as compliant to GDPR, processing and storing data securely within the EU only. Contracts with these providers are held by the DPO. A2O also shares data which is processed outside of the organisation, by government bodies such as HMRC, Local Authority, Department for Education etc. This processing is required under law and legislation.

Compliance


Compliance with the Act is the responsibility of all staff, paid or unpaid. A2O will regard any unlawful breach by any staff, paid or unpaid, as a serious matter which will result in disciplinary action. Any such breach could also lead to criminal prosecution. Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

Complaints

In the event that a data subject or organisation have concerns or cause to complain about the manner in which we process data, they are able to contact the DPO directly and/or ask the Information Commissioner to assess our compliance (ICO.org.uk), as stated on all A2O Privacy Notices.

A copy of this policy can be obtained from the Nursery Offices or downloaded via our website:

www.acorns2oaksnurseries.net/home/policies

| | | |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Reviewed by: Beverley Noble | Signed:  | Date: Sept 2020 Review: Sept 2021 |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------|

APPENDIX A – EYFS 2017 record keeping legal requirements

The Early Years Foundation Stage (EYFS) 2017 states that the legal requirements around record keeping are:

3.68 Providers must maintain records and obtain and share information (with parents and carers, other professionals working with the child, the police, social services and Ofsted or the childminder agency with which they are registered, as appropriate) to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met. Providers must enable a regular two-way flow of information with parents and/or carers, and between providers, if a child is attending more than one setting. If requested, providers should incorporate parents' and/or carers' comments into children's records.

3.69. Records must be easily accessible and available (with prior agreement from Ofsted or the childminder agency with which they are registered, these may be kept securely off the premises). Confidential information and records about staff and children must be held securely and only accessible and available to those who have a right or professional need to see them. Providers must be aware of their responsibilities under the Data Protection Act (DPA) 1998 and where relevant the Freedom of Information Act 2000.

3.70. Providers must ensure that all staff understand the need to protect the privacy of the children in their care as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

3.71 Records relating to individual children must be retained for a reasonable period of time after they have left the provision (footnote 56: individual providers should determine how long to retain records relating to individual children)

APPENDIX B – Data Retention Schedules
EXECUTIVE OFFICE
Personnel Records

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------|------------|
| Personnel files | Personal & sensitive data. Training, supervision, working hours & disciplinary records. | Paper based locked cabinets | 6 years after employment ceases | Recommendation: CIPD | Electronic |
| | Records of founded or unfounded allegations of a child protection nature. Allegations found to be malicious must be removed from files. | | Until the person's normal retirement age or 10 years after the date of the allegation | Requirement: Keeping Children Safe in Education, DfE 2016 | Electronic |
| Unsuccessful applicants | Personal data. Application forms and interview notes. | | 6 to 12 months after interview | Recommendation: CIPD | None |
| Redundancy cases | Personal data. Calculations & HMRC correspondence | | 7 years from the date of redundancy | Requirement: HMRC Recommendation: CIPD | Electronic |
| Payroll records | Salary records, SMP, SSP, Parental leave, PAYE, NIC, Pensions, | Paper based locked cabinets Accounting s/ware | 6 years | Requirement: HMRC Recommendation: CIPD | Electronic |
| DBS check information | Personal data. Providers must maintain: Subject name, cert date & URN, position applied & decision. | Electronic database | Certificate is kept for duration of employment | Recommendation: DBS, Ofsted and LADO | None |

Governance & Data Protection

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|-------------------------------------------------|------------------------------|----------------------------|-------------------------------------------------|------------------------------------|--------------------------|
| Persons with Significant Control (PSC) Register | Personal Data | Electronic and paper based | Until trusteeship ends | Requirement: CO Act | None |
| Data Protection Register | Breaches and Access Requests | Electronic | Indefinite | Requirement: GDPR | Electronic |
| DBS check information | Personal data. | Electronic database | Certificate is kept for duration of Trusteeship | Recommendation: DBS, Ofsted & LADO | None |
| Minutes/minute book | Minute Book | Paper based | At least 10 years from date of meeting | Requirement: CO Act | Electronic typed version |
| | Typed minutes | Electronic | Permanently | Recommendation: CIPD | Electronic |

Health and Safety

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------------------------------------------|----------------------|----------------|
| Accidents | Staff accidents | Accident book | 3 years after last entry | Requirement: DWP | Locked archive |
| | COSHH Incidents | Accident book | 40 years after last entry | Requirement: COSHH | Locked archive |
| | Records of any reportable death, injury, disease or dangerous occurrence | Accident book Archived in Safe | 3 years from the date the record was made | Requirement: RIDDOR | Locked archive |
| | Assessments under Health & Safety Regulations and records of consultations with safety representatives and committees | Paper based locked cabinets. | Permanently | Recommendation: CIPD | Electronic |
| Risk Assessments | Assessments of hazards and risks | Paper based | 3 years for new buildings, archived indefinitely for older buildings. | Recommendation: CIPD | Electronic |

Finance & Administration

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|---------------------------------------|-------------------------------------|----------------------------|----------------------------------------------------------|------------------------------|-----------------------------------------|
| Accounting records | Invoices, receipts, bank statements | Paper based | 6 years from end of financial year | Requirement: CH Act & CO Act | Electronic |
| Employers liability insurance records | Insurance policy and schedule | Paper based | 40 years from the date insurance commences or is renewed | Recommendation: HSE | Electronic |
| Policy documents | | Electronic and Paper based | Life to policy then 3 years thereafter | Recommendation: IRMS | Electronic |
| Visitors book/signing in sheets | | Paper based | 24 years as Child Protection trail | Recommendation: IRMS | Electronically where possible or locked |
| Complaints records | | Electronic and paper based | At least 6 years after complaint is resolved | Recommendation: IRMS | Electronically where possible or locked |

YOUTH CLUB

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|-------------------------|-----------------------------------------|-------------------------------------------------|-------------------------------|---------------------|-----------------------------------------|
| Consent Forms | Personal & sensitive data | Paper based | 6 months from last attendance | GDPR guidance | Electronic |
| Accidents | Young Person Accidents | Paper based | 24 years | Recommendation: HSE | Electronically where possible or locked |
| | Staff, COSHH, RIDDOR or HSE Assessments | See Executive Office Health and Safety schedule | | | |
| Photographs | Website or newsletters | Electronic | 6 months from last attendance | GDPR guidance | None |
| Registers of Attendance | Full name only | Electronic database | 3 years | | Electronic |
| Safeguarding Incidents | Concerns/reports | Paper/electronic | 24 years | LSCB | Electronic |

SERVICE USERS & PROVIDERS

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|-----------------------------|--------------------------------|---------------------|------------------------------------------------------------|------------------------------------|------------------------|
| Hall booking forms | Personal data and bank details | Paper based | Immediately after booking is complete and deposit returned | Requirement: GDPR | None |
| Liability insurance records | Insurance policy and schedule | Paper based | 40 years from the date insurance commences or is renewed | Recommendation: HSE | Electronically archive |
| DBS check information | Personal data. | Electronic database | Certificate kept for duration of Involvement | Recommendation: DBS, Ofsted & LADO | None |

ABCD COMMUNITY CONTACTS

| Information | Details | Storage | Retention Period | Status & Authority | Archive |
|-----------------------------|-------------------------------|------------------------------|----------------------------------------------|-----------------------------------|------------|
| Contact Database | Personal Data | Locked phones and electronic | 1 year after end of contract | Recommendation: GDPR | Electronic |
| Liability insurance records | Insurance policy and schedule | Paper based | 40 years from start or renewal | Recommendation: HSE | Electronic |
| DBS check information | Personal data. | Electronic database | Certificate kept for duration of Involvement | Recommendation: DBS, Ofsted, LADO | None |

CHILDCARE SETTINGS

- Paper based data is kept throughout attendance at setting – this is a statutory requirement of EYFS, CC Act, Ofsted and LSCB
- Upon leaving, only records required by law or legislation are electronically archived. All others are disposed through confidential shredding.
- A concise register of files is to be maintained with respective disposal dates.

| Information | Details | Retention Period | Status & Authority | Archive |
|--------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------|------------------------------------------------------------------|
| Children's records (including admission pack) | Contact details | 3 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted | Electronically and within 1 term after leaving the setting |
| | Consent Forms | 3 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted | |
| | Child Protection (CP)/Safeguarding | 24 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted, LSCB | |
| | SEND, Care Plans, Referrals | 24 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted | |
| | Accident log | 24 years after leaving the setting | Recommendation: Limitation Act 1980 | |
| | Records of any reportable death, injury, disease or dangerous occurrence | 3 years after the date the record was made, 24 years if relating to CP | Requirement: RIDDOR | |
| | Register of non-attendance | 24 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted, LSCB | |
| | Medical Information | 3 years after leaving the setting, 24 years where SEND, CP or accident records exist | Requirement: EYFS, CC Act, Ofsted, LSCB | |
| | Allergy Information | 3 years after leaving the setting, 24 years where CP or accident records exist | Recommendation: Limitation Act 1980 | |
| | Care Cost Agreement | Upon leaving the setting, once fees are settled. | | None |
| Early Years Funding Paperwork | Upon leaving the setting | | None | |

| | | | | |
|--------------------|--------------------------------------------------------------|-----------------------------------|--------------------------------------|------------------------------------------------------------|
| Playroom Documents | Registers – Full name & DOB | 3 years after leaving the setting | Requirement: EYFS, CC Act, Ofsted | Electronically and within 1 term after leaving the setting |
| | Emergency Contacts – First name & 2 x phone numbers | Upon leaving Setting | Requirement: EYFS, CC Act, Ofsted | None |
| | Medicine Consent Forms – Full Name, DOB, Medical Information | Upon leaving Setting | Requirement: EYFS, CC Act, Ofsted | None |
| | Allergy Charts – Full name & Photo | Upon leaving Setting | Requirement: EYFS, CC Act, Ofsted | None |
| | Diet requirements & Lunch Charts – Full name & Photo | Upon leaving Setting | Requirement: EYFS, CC Act, Ofsted | None |

| | | | | |
|-------------------|--------------------------------------|-----------------------------------------------------------------|--------------------------------------|-----------------------------------------|
| Learning Journals | Full Name, DOB, Photo, Referrals | Upon leaving Setting – Given to Parents or next setting/school. | Requirement: EYFS, CC Act, Ofsted | None |
| Photographs | On website and displayed in Settings | Upon leaving Setting | Recommendation: GDPR | None |
| Staff Registers | Full name only | 3 years from end of academic year | Recommendation: GDPR | Electronic at end of each academic year |

| Abbreviation | Accredited Body |
|--------------|--------------------------------------------------|
| CIPD | Chartered Institute of Personnel and Development |
| DBS | Disclosure and Barring Service |
| DfE | Department for Education |
| HMRC | Her Majesty's Revenue and Customs |
| | Health and Safety Executive |
| IRMS | Information and Records Management Society |
| LSCB | Local Safeguarding Children's Board |
| LADO | Local Authority Designated Officer |

| Abbreviation | Law or Legislation |
|--------------|----------------------------------------------------------------------------|
| CC Act | Childcare Act 2006 |
| CH Act | Charity Act 2011 |
| CO Act | Companies Act 2006 |
| COSHH | Control of Substances Hazardous to Health Regulations 2002 |
| EYFS | Early Years Foundation Stage Statutory Framework 2017 |
| GDPR | General Data Protection Regulations 2018 |
| RIDDOR | Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 |
| | |