Policy:	Data Protection
Last Review Date:	30/06/20
Next Review Date:	30/06/21
Lead:	Head of Resourcing

Data Protection Policy

Introduction

Real Ideas Organisation CIC (Real Ideas) and its subsidiaries is fully committed to compliance with the requirements of the Data Protection Act 2018 (DPA), and other data protection legislation including the General Data Protection Regulation (GDPR).

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our company and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; customers; members; suppliers; business contacts and other people and organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the DPA.

This policy is not contractual but indicates how Real Ideas intends to meet its legal responsibilities for data protection.

Scope of this policy

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access during their work. This policy requires staff to ensure that the Data Controller (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

This policy applies to all employees, workers and volunteers, irrespective of their work base (and therefore including those who work from home) who handle personal data, whether this relates to their colleagues, customers, suppliers, business contacts or anyone else. A copy of this policy will also be given to any third parties to whom we outsource any data processing.

Definitions

Business The purposes for which personal data may be used by us:

purposes	Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include (without limitation) the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or regarding legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as managing membership, recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, members, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special category data	Personal data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data, data concerning health, sex life and sexual orientation, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Legal considerations

This policy has been drafted to take account of our obligations under the Data Protection Act 2018 , the GDPR and related legislation. Any codes of practice or advisory notes issued by the Information Commissioner should also be noted.

Principles

We endorse and adhere to the data protection principles of the DPA which are summarised as follows:

Personal data must:

1. be processed lawfully, fairly and transparently;
2. be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with those purposes;
3. be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected;
4. be accurate and, where necessary, kept up to date;
5. only be kept for as long as is necessary for the purpose for which it was collected;
6. be kept in a manner that ensures appropriate security of the personal data including against unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
7. not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and workers of Real Ideas who obtain, handle, process, transport and store personal data for us must adhere to these principles always.

Handling of personal data

Real Ideas will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- make it easy for data subjects to update the information we hold about them
- take steps to always ensure the accuracy of information used
- not keep information for longer than required (operationally or legally)
- take steps to safeguard personal information by physical, technical means and organisational measures (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems using secure passwords which are robust and changed periodically; and ensuring that individual passwords are not easily compromised)
- ensure that personal information is not transferred outside the EEA without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, Real Ideas will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the designated Data Protection Office or DPO) - currently the Head of Resourcing
- a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously
- methods of handling personal information are regularly assessed and evaluated
- any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing, and including appropriate safeguards for the data subjects
- any disclosure of personal data will follow approved procedures.

Real Ideas also has a legal obligation to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings (Protection of Employment) Regulations (TUPE).

Special Category Data

In most cases where we process special category data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance and Your Rights

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

If you wish to exercise any of the rights set out above, please contact the Data Protection Officer (datacontroller@realideas.org)].

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform HR@realideas.org so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Responsibilities

Everyone who works for or with Real Ideas has responsibility for ensuring data is collected, stored, processed and handled appropriately.

However, people with key areas of responsibility within Real Ideas are:

- The **Real Ideas Leadership Team** are ultimately responsible for ensuring that Real Ideas meets its legal obligations.

- Data Protection Officers are responsible for:
    - Keeping Leadership and non-exec Directors updated about data protection responsibilities, risks and issues
    - Ensuring that all those who manage and handle personal information understand that they are responsible for following good data protection practice
    - Arranging data protection training and guidance for those who manage and handle personal information
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Real Ideas holds about them (called "subject access requests")
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Managed Service Provider** is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services, the company is using to store or process data, for instance cloud computing services.

- The **Head of Marketing** is responsible for:

    - Approving any data protection statements attached to communications such as emails and letters

- Addressing any data protection queries from journalists or media outlets, such as newspapers
- Ensuring marketing databases are checked against industry suppression files every six months
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Employee responsibilities

All employees must ensure that, in carrying out their duties, Real Ideas is able to comply with its obligations under the DPA. In addition, each employee is responsible for:

- checking that any personal data that he/she provides to us is accurate and up to date
- informing us of any changes to information previously provided, e.g. change of home or email address or phone number, marital status or civil partnership, bank details etc
- checking any information that we may send out from time to time, giving details of information that is being kept and processed
- ensuring that if, as part of their responsibilities, they collect information about other people or about other employees, they comply with this policy. This includes ensuring that information is processed in accordance with the DPA, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are reminded that the DPA does not just apply to records relating to our employees, but also to the records of any customers, members and suppliers that we work with. The information stored should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or saved electronically (for example in emails, current or deleted) are potentially disclosable in the event of a request from an employee, supplier or customer.

Employee records

We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, employment history with Real Ideas, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally or otherwise).

This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations.

We also process information relating to employees' health, some of which may fall under the definition of 'special category data'. This typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms); DSE assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations.

From time to time we may ask employees to review and update the personal information we hold about them. We will normally send a copy of his/her basic personal data to each employee annually. Employees should check this information carefully and inform us of any inaccuracies. However, we ask that employees do not wait until asked to update this information but inform us immediately of any notable change(s).

Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All hard copy Real Ideas personnel files are kept in a locked cabinet at Devonport Guildhall and are not to be removed from there. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.

Programme Leads and Line Managers have access to the personnel records of the employees that they support, but not to the files of other employees. Programme Leads/Line Managers are required not to retain their own copies of personal data, but to use our central storage system. Copies of supervision / 1:1 records, appraisal forms and other notes e.g. day to day management discussions can be held locally by the Programme Leads/Line Managers, if the records are kept securely.

Portable devices that are removed from our premises, such as laptops, smartphones and any other electronic equipment, should never have data saved directly to them unless access to the servers isn't possible. Portable devices must be protected by a password or access code to prevent unauthorised access, and the data encrypted and protected by a password or access code.

All employees and workers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body).

Third party processors (e.g. Payroll) will be required to provide sufficient guarantees for their data security measures and compliance with them. A written contract will be in place with each supplier

which requires them to dispose of data securely and to provide suitable evidence of this. Checks will be made to ensure that secure data disposal facilities are in place and regular monitoring will take place.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords. We encourage all staff to use a password manager to create and store their passwords.
- No personal data is to be stored on any removable media, unless such media is fully encrypted
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones**.**
- Storage of data on mobile devices, will only be permitted if such devices are subject to O365 security management (including privately owned devices)
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Publication of information

Information may be contained within externally circulated publications such as brochures and other sales and marketing literature or included on our website.

Any individual who wishes his/her details not to be included in such publications should contact the relevant Programme Lead/ Head of Marketing or the DPO.

Subject access requests

Please note that under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the DPO if you would like to correct or request information that we hold about you.

Real Ideas takes step to ensure that individuals are aware that their data is being processed and that they understand how the data is used, and how to exercise their rights under the DPA

To these ends, Real Ideas has a privacy policy setting out how we use data relating to individuals. This is publicly available via the Real Ideas website.

All individuals who are the subject of personal data held by us are entitled to:

- ask what information we hold about them and why
- ask how to gain access to it
- be informed of how to keep it up to date
- have inaccurate personal data corrected or removed
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance
- be informed what we are doing to comply with our obligations under the DPA.

This right is subject to certain exemptions which are set out in the Act.

Any person who wishes to exercise this right should make a request in writing to the Head of Resourcing or via email to datacontroller@realideas.org. A copy of the information will be provided free of charge however Real Ideas reserves the right to charge a reasonable fee to cover administrative costs when a request is manifestly unfounded or excessive, particularly if it is repetitive. Real Ideas may also charge a reasonable fee to comply with requests for further copies of the same information.

If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Information must under no circumstances be sent outside of the UK without the prior permission of the Head of Resourcing.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that this is provided within one month of receipt of a written request unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

Processing Employee Data

We may need to process the personal data of employees for the purposes of administration, managing and employing them. This includes payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision,

recruitment, family policies (maternity, paternity, adoption, shared parental leave etc) and equal opportunity monitoring.

Information about an individual will only be kept for the purpose for which it was originally provided. Employees must not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed or they have expressly consented to being contacted in this way for direct marketing purposes.

Please contact the DPO or Head of Marketing for advice on direct marketing before starting any new direct marketing activity.

Retention and disposal of data

Information will be kept in line with our document retention guidelines (Appendix 1 & 2). All employees are responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin). Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

Registration

The DPA requires every data controller who is processing personal data, to notify and to renew their notification on an annual basis. Failure to do so is a criminal offence.

Real Ideas is registered in the Information Commissioner's public register of data controllers. The Head of Resourcing is our DPO and is responsible for ensuring compliance with the DPA, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of Real Ideas.

Any changes made to the information stored and processed must be brought to the attention of the Head of Resourcing immediately.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	
How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Details of transfers to third country and safeguards	
Retention period	

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of special category data, and will ensure any biometric and genetic data is considered special category.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects or other projects that may affect the processing of personal data commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the DPO. Transfers outside the EEA must be subject to additional safeguards as outlined in our privacy policy.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either alone or as part of a pattern of failures

Monitoring

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

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Implementation, monitoring and review of this policy

The Head of Resourcing has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation and whenever there are relevant changes in legislation or to our working practices.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the PDC. Any breach will be taken seriously and may result in formal disciplinary action. Any employee or worker who considers that the policy has been breached in any way should raise the matter with their manager or the Head of Resourcing.

Appendix 1 – Document storage guidelines

These guidelines describe how and where data should be safely stored. Employees should keep all data secure, by taking sensible precautions and following these guidelines.

Questions about storing data safely can be directed to the DPO.

General

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- The only people able to access data covered by the Data Protection Policy should be those who **need it for their work**.
- Data **should not be shared informally**. Particular care should be taken when sharing any data by email. Whenever data is to be sent by email that contains (i) large amounts of data or (ii) data that contains special category data or (iii) data that would (on a reasonable assessment) present a high risk to the rights and freedoms of individuals if it was lost, destroyed, or otherwise intercepted, email encryption functionality should be used. This is available to all staff members. When access to confidential information is required, employees can request it from HR@realideas.
- Personal data **should not be disclosed** to unauthorised people, either within the organisation or externally.
- When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**, or **shredded** and disposed of securely when no longer required.
- Data should be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- Any employee who discovers personal or special category data in an inappropriate place (for example unknowingly sent to the wrong printer) should immediately pass this to the Head of Resourcing, ensuring that its contents are not revealed to anyone else.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared

between employees. Strong passwords are at least 8 characters long and contain a mix of upper case and lower-case letters, as well as numbers.

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used. Data stored on external USB drives should be encrypted.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Where personal electronic devices are used to access and/or store Real Ideas data, such devices must comply with all Real Ideas policies, including the Data Protection Policy. As such, for the purposes of data protection, such devices will be treated as if they are Real Ideas property.
- All servers and computers containing data should be protected by **security software and a firewall**.
- When working with electronic personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Data must be **encrypted before being transferred electronically**. The Head of IT can explain how to send data to authorised external contacts.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data. This is especially true for employees using home computers to access Real Ideas resources via VPN.

Appendix 2 – Document retention periods

Documents	Minimum recommended retention period	Authority/comments
HR records		
Employee personnel & training files	Six years after employment ceases	Limitation Act 1980 Health and safety training records may need to be kept longer (see below)
Unsuccessful job applications - forms and interview notes	6 months - 1 year following date of appointment	Three months for a tribunal claim on grounds of discrimination (although this may be extended if the tribunal considers this to be 'just and equitable'). One-year limitation for defamation actions.
Time cards/records	Two years following audit	Working Time Regulations 1998
Flexible working requests	Six years after leaving	Limitation Act 1980
Expense accounts	Six years following year end for public companies	Companies Act 1985, section 222 as modified by the Companies Act 1989 and Companies Act 2006
Sickness records	Forty years after employment ends	In case of claims for personal injury or under the Equality Act 2010
Statutory sick pay records	Three years after end of tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982
Leave records, including annual leave, compassionate leave, time off for public duties or for dependants	Two years	
Appraisals	Two years	
Discipline and grievance records	In most cases may not be used once warnings are spent but should be retained for two years	Transfer of Undertakings (Protection of Employment) Regulations 2006
Maternity leave and pay records	Three years after end of tax year in which the maternity period ends	Statutory Maternity Pay (General) Regulations 1986 and Maternity & Parental Leave Regulations 1999

Adoption leave and matching certificate	Three years after end of tax year in which the adoption period ends	Maternity & Parental Leave Regulations 1999
Paternity leave and pay records	Three years after end of tax year in which the paternity period ends	Maternity & Parental Leave Regulations 1999
Parental leave	Five years from first request (eighteen years for disabled child)	Best practice
Details of redundancy calculations, payments, HR1	Six years after employment ceases	Best practice
Redundancy correspondence	Six years after employment ceases	Best practice
Redundancy - less than 20 - facts relating to this	Three years	Limitation Act 1980
Redundancy - more than 20 - facts relating to this	Twelve years	Limitation Act 1980
Documents proving the right to work in the UK	Two years after employment ceases	Best practice

Pensions		
Records relating to notifiable events and concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	Six years from the end of the scheme year in which the event took place or the date upon which the accounts/reports were signed/completed	Retirement Benefits Schemes (Information Powers) Regulations 1995
Pension scheme investment policies	Twelve years from the ending of any benefit payable under the policy	Best practice
Actuarial valuation reports	Twelve years after benefit ceases	Best practice
Money purchase details	Six years after transfer or value taken	
Trust deeds and rules	Permanently	Best practice

Health & Safety		

Accident books, records and reports	Forty years	Three years from date of last entry for claims under F2508(revised); longer period recommended because of risk of personal injury claims or claims under the Equality Act 2010
Health and safety records	Forty years	Personal injury claims must normally commence within three years of injury. However, this period may be substantially extended for industrial injuries which are not capable of being detected in less than three years.
Risk assessments and records of consultations with safety reps and committees	Permanently	Best practice
Statutory and Regulatory Training	Six years after leaving	Limitation Act 1980
First Aid Training	Six years after leaving	Health and Safety (First-Aid) Regulations 1981
Fire Warden Training	Six years after leaving	Fire Precautions (Workplace) Regulations 1997
H&S representatives training	Five years after leaving	Health & Safety (Consultation with employees) Regulations 1996
H&S training - employees	Five years after leaving	H&S Information for Employees Regulations 1989

Medical records		
Medical reports (general)	6 years after leaving	Access to Medical Reports Act 1988
Medical records as specified by COSHH regulations	Forty years from date of last entry	Control of Substances Hazardous to Health Regulations 2002
Records of tests and examinations of control systems and protective equipment under the COSHH regulations	Five years from date of the test	Control of Substances Hazardous to Health Regulations 2002

Accounting records		

Accounting records	Three years for private companies, six years for plc.	Companies Act 1985 section 221, as modified by the Companies Act 1989 and Companies Act 2006
HM Revenue & Customs approvals	Permanently	Best practice
Wage/salary records (including overtime, bonuses and expenses, other payment records including statutory payments, working tax credit, payments to subcontractors, gains on share options and student loan deductions)	Six years following year end	Taxes Management Act 1970 Income Tax (Employments) Regulations 1993 and Income Tax (Pay As You Earn) Regulations 2003
National Minimum Wage	Three years after the end of the tax year which the NMW records cover	National Minimum Wage Act 1998

Appendix 3: Data Controllers and Data Processors

The DPA draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the data controller that must exercise control over the processing and carry data protection responsibility for it.

Role: Data Controller

Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed within the Real Ideas context this is more often than not the Contract Manager in association with the Head of Resourcing

The Data Controller exercises overall control over the 'why' and the 'how' of a data processing activity (although this may also be dictated by funders).

The following decisions can only be taken by the Data Controller:

- to collect the personal data in the first place and the legal basis for doing so;
- which items of personal data to collect, i.e. the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data

Role: Data Processor

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. This can be any member of Real Ideas staff, particularly although not exclusively administrators.

This is why it's imperative that all staff are familiar with Data Protection regulations and GDPR (General Data Protection Regulations).

Within the terms of the agreement with the data controller, and its contract, a data processor may decide:

• what IT systems or other methods to use to collect personal data;

• how to store the personal data; the detail of the security surrounding the personal data;

• the means used to transfer the personal data from one organisation to another;

• the means used to retrieve personal data about certain individuals; the method for ensuring a retention schedule is adhered to; and

• the means used to delete or dispose of the data

Processing, in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data,

b) retrieval, consultation or use of the information or data,

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

d) alignment, combination, blocking, erasure or destruction of the information or data

Staff have a responsibility to ensure that they are compliant with all aspects of the DPA, the GDPR and Real Ideas policies and procedures relating to data protection and privacy.

GDPR incorporates many of the principles within the earlier Data Protection Act 1998, but puts additional emphasis on the protection of personal data, explicit consent, the right to be forgotten, and portability. Further information can be obtained from the Information Commissioners Officer or Head of Resourcing or DPO.