Information Governance Framework

April 2025

Date	April 2025
Planned Review Date	April 2028
Reactive Review Date & Reason	
Revised Review Date	
Author (Job Title)	Head of Cyber Security & Data Compliance
Owner (Job Title)	Director of IT, Cyber and Data Security
Directorate	IT, Data & Cyber Security

Policy Review History

Version	Action & Changes	Author	Date
2	All DPA 1998 legislation information changed to GDPR and DPA 2018. Three new sections on Mobile and Tracking Devices, CCTV and Remote/Home working. ICT security section removed and is included in ICT Security policy.	LM	March 2019
3	4.2.2 Classifications of emails removed as all emails are now encrypted. 4.2.6 Removed section on the Group mainly relying on consent. Contract and legitimate interests are the main lawful basis Thirteen rely on.	LM	April 2022
4	Moved over to new framework template.	LM / JW	April 2025

Governance Information

Equality and Diversity	Initial screening indicated no adverse impact on any of the protected characteristics
Customer Involvement and Consultation	Reviewed by Customer Involvement, feedback received, and acknowledge and responded too.
Environmental Sustainability	No issues/implications affecting environmental sustainability.
Monitoring and Review	The Data Compliance Manager within Thirteen will review the policy every three years or sooner if there are any legislative or regulatory changes
Responsibility	Data Compliance Manager will be responsible for the overall implementation of the policy.

1 REFERENCE MATERIAL

1.1 The main legislation relating to Information Governance and have been used when developing this framework:

- General Data Protection Regulation 2018 (GDPR 2018)
- Data Protection Act 2018 (DPA 2018)
- Co-operative and Community Benefit Societies Act 2014
- Guidance from the Information Commissioner's Office (ICO) website
- Data Protection Good Practice Guidance
- Acceptable Use Policy
- Building Support Services – CCTV procedure
- Social Housing Regulation Act
- Social Tennant Access to Information Requirements (STAIRs) consultation

2 WHY WE NEED THIS FRAMEWORK

2.1 To operate an efficient and effective business to the benefit of our customers and colleagues and their diverse needs whilst meeting our legal and regulatory requirements.

2.2 Thirteen Group and its partner companies need to collect, use, and hold information about people to operate effectively and efficiently and ensure that services appropriate to the needs of employees, customers, Board Directors, and representatives are provided.

2.3 This information may be sensitive and/or highly sensitive, and maybe collected, recorded, and stored both manually on paper and/or electronically. It is vital that any information, however it is collected or stored, is dealt with lawfully and correctly and there are safeguards in place in the General Data Protection Regulation 2018 and the Data Protection Act 2018 to ensure this.

2.4 This framework aims to detail the organisational and legislative requirements with regards to the following:

- Data Protection;
- Confidentiality;
- Access to information; and
- Document management.

2.5 The need to adhere to this framework and associated policies is included in both the terms and conditions of staff employment and the Code of Conduct applicable to all staff, Board Directors, and representatives of Thirteen. Any breaches will be investigated and where a serious breach has occurred disciplinary action may be taken.

2.6 This framework has been written to help us achieve our visions and strategic objectives.

3 HOW WE DO THIS

3.1 Data Protection

3.1.1 The GDPR and DPA 2018 establishes a framework of rights and duties which are designed to safeguard personal data. The framework specifies six lawful bases for processing data which balances the legitimate needs of Thirteen to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

Lawful bases
Lawful basis 1: Consent
Lawful basis 2: Contract
Lawful basis 3: Legal Obligation
Lawful basis 4: Vital Interests
Lawful basis 5: Public Task
Lawful basis 6: Legitimate Interests

The legislation itself is complex, but is underpinned by a set of seven straightforward, common-sense principles in Article 5 that require that data must be processed with:

Principles

Principle 1: Lawfulness, fairness, and transparency
Principle 2: Purpose limitation
Principle 3: Data minimisation
Principle 4: Accuracy
Principle 5: Storage limitation
Principle 6: Integrity and confidentiality (security)
Principle 7: Accountability

The regulation also specifies the following rights for individuals which the organisation must adhere to:

Rights

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

3.1.2 These principles must be followed by anyone processing personal data. More detailed information regarding the principles is attached at Section 2 of the supporting documentation and how we process your personal data can also be seen in our privacy notice.

3.1.3 Use of Employee Protection Register / Concerns Markers

We have a duty under the Health and Safety Act 1974 to provide a safe working environment for its employees and representatives. As many employees come into direct face-to-face contact with customers and clients as part of their work, in situations which are sometimes volatile or that may present other risks to the safety of staff. Thirteen Group therefore recognises the necessity of using an Employee Protection Register / Concerns. However, while sensitive personal data may be used and stored to support inclusion in the register, it will not be included in the Employee Protection Register / Concerns Marker and therefore usage of the Employee Protection Register / Concerns Marker complies with the GDPR and DPA 2018.

3.1.4 Data Sharing/Processing Agreements

Employees, representatives, and Board Directors working for and on behalf of Thirteen Group must understand the importance of good practice when dealing with personal and sensitive personal data held in customer records and appreciate the rules by which individuals' data may be accessed and processed. Thirteen Group expects that data held by the organisation or any companies acting on behalf of the Group, will always be treated as confidential and will be

processed in accordance with the GDPR 2018, DPA 2018 and Thirteen Group's other policies and procedures. Data will not be made available to third parties for commercial or marketing purposes. Organisations using any type of data held by Thirteen Group will have to sign a data sharing/processing agreement or contract and be bound by the requirements of that agreement.

3.1.5 Data Security Breaches

A data security breach can happen for numerous reasons, for example: loss or theft of equipment on which data is stored; unauthorised access or disclosure; equipment failure; human error; and fire or flood. If a potential breach is identified action will be taken to ensure the matter is contained and if possible, the information recovered; an assessment of ongoing risk is made; there is notification of the breach to the affected parties as required; and an evaluation of the effects of the breach and the response. Action may include disciplinary investigations if employees are involved. Where data breaches are reportable to the ICO they must be reported within 72 hours of the organisation becoming aware of the breach.

3.2 Confidentiality

3.2.1 The Group are aware of its responsibilities when using or handling confidential information. There is a requirement that employees, Board Directors, and representatives of Thirteen shall not misuse any information or allow others to do so. Confidential information must be used, processed, and handled in accordance with this framework; Thirteen Group's other policies and procedures; the GDPR 2018 and the DPA 2018.

3.2.2 Sharing Confidential Information between Employees, Representatives and Board Directors

Within Thirteen Group, confidential information should only be available to employees, representatives and Board Directors who genuinely need to know this information to carry out their work effectively. Confidential information should only be shared with the necessary and appropriate employees, representatives, and Board Directors. Where confidential information is shared to an entire team, care should be taken to ensure that there is a legitimate need for the entire team to have access.

3.2.3 Confidential Correspondence

Employees, representatives and Board Directors will have access to confidential correspondence and should exercise care and caution when handling correspondence received into Thirteen Group, i.e. envelopes, marked 'confidential', 'personal', 'sensitive' or 'highly sensitive' should be handled in accordance with administration procedures, policies, the GDPR 2018 and DPA 2018.

3.2.4 Multi-Agency Partnerships

Thirteen Group recognises the necessity of working with other agencies so that we can meet the needs of customers, clients or prospective customers and clients so that employees, representatives, and Board Directors can carry out their work effectively. The Group will aim to maintain a balance between the need for confidentiality and the sharing of information necessary to make an effective response to other agencies' requesting information. Employees, representatives, and Board Directors should only share information with other agencies on a need-to-know basis, when there is a lawful basis for doing so. Also refer to section 4.1.4 (Data-Sharing Agreements) of this framework.

3.2.5 Anonymous Information

Where employees, representatives or Board Directors of the Group are given information from anonymous sources the information will be passed to the relevant team for reference, or where appropriate, take action to investigate any allegations that may be included within the information. All employees, Board Directors, and representatives of Thirteen are required to ensure that personal information gained from an anonymous source remains confidential.

3.2.6 Disclosure of Confidential Information

Where requests are made for the disclosure of personal information employees, representatives and Board Directors must consider whether the consent of the individual concerned should be sought or if another lawful basis can be relied upon.

The GDPR 2018 and DPA 2018 reinforces the Crime and Disorder Act 1998 in that it allows for the disclosure of personal information, where the disclosure is for the purposes of the prevention and detection of crime, or the apprehension or prosecution of offenders; and where failure to disclose would prejudice those objectives.

3.2.7 Breaches of Confidential data

All Thirteen Group employees, representatives and Board Directors have a duty of care to ensure that personal information remains confidential. Discussing customers, clients, former customers, or clients, rehousing applicants, or other employees in public places, on social media or in an unprofessional context is unacceptable. Customers, clients, contractors, employees, representatives, and Board Directors are all expected to respect the rights of others to confidentiality and privacy of their information. Although the Group recognises that most breaches of confidential data occur not out of malice but through thoughtlessness and lack of awareness of the consequences of an action. Any breach of confidential data will be considered a serious issue, and this could be

regarded as gross misconduct where following investigation evidence shows that there has been a breach of the GDPR, or confidential company information has been shared.

3.3 Access to Information

Thirteen Group facilitates people's right to see what information is kept about them, and fully endorses the principles of data protection, as specified in the GDPR 2018 and DPA 2018 and other related legislation. Requests for information will be processed within the requirements of the Act and the data subject access procedure followed when requests are received.

3.3.1 Freedom of Information

The Freedom of Information Act 2000 gives any individual, regardless of age, nationality, or residence the right to access recorded information held by public sector organisations, as a registered society under the Co-operative and Community Benefit Societies Act 2014, Thirteen Group is not obliged to meet with the requirements of this act however, as a commitment to being open and transparent the Group will consider reasonable requests for information and where possible allow information requesters to know where they may find the information for themselves when we are not obliged to provide the information.

3.3.2 Data Subject Access Request

In accordance with the GDPR 2018, applicants / former and current customers / clients, employees, former employees, and representatives have a right to know what personal information Thirteen Group holds about them; what we use the information for and to whom we have disclosed that information or to whom we may disclose that information to. This applies to information held in Thirteen Group's computer records and manual files. Individuals can therefore make a request for their personal information through our website (Click Here), via email or phone and in line with our Data Subject Access Request Procedure.

3.3.3 Social Tennant Access to Information Requirements (STAIRs)

This includes any information identified with the Social Tenant Access Information Requirements (STAIRs), where social tenant and their representatives to access information to the management of their housing. This regulation is currently out for consultation, and we are ensuring we meet the requirements of STAIRs once the consultation is finalised.

3.3.4 Accuracy of Personal Data

Applicants / former and current customers / clients, employees and representatives have a right to request that information held by the Group, which they believe is inaccurate is corrected or removed. Principle 4 of the GDPR requires accuracy and one of the rights of the GDPR is the right to rectification which we will seek to facilitate. If the information is not amended for a justifiable reason, the Group will provide an explanation as to why this has been decided. If the individual, then disagrees with the decision this will be recorded.

3.3.5 Third Party Requests for Information

Occasions may occur where third parties contact the Group to request information relating to applicants / former or current customers / clients. Where this is the case third-party consent to share this information must be received, or an informed decision be made to allow the information to be released without consent where there is a lawful basis for doing so. This includes requests from relatives, other agencies, local authority councillors, MPs, and Board Directors.

3.3.6 Safeguarding and Prevention of Crime

We are legally obliged to share information, appropriately with the relevant agencies (i.e. police, health, and social services), when we believe that a client, customer, or anyone else is at risk of harm, in order to prevent a crime, or to assist in the detection of a crime. Further information can be found in the Group Safeguarding Adults and Safeguarding Children policies and procedures.

3.4 Document Management

We manage all documents and records created or received, using a reliable and well-designed system which describes the standards of practice the Group requires to manage and dispose of records. More information can be seen in our acceptable use policy, regarding how colleagues care for personal data.

3.4.1 Electronic Document and Records Management

Thirteen Group endorses the use of electronic document and records management and expects employees and Board Directors to manage documents and records electronically wherever and whenever possible.

3.4.2 Document Retention

A records retention schedule document is in place which sets out the categories of records the Group retains and the length of time these records need to be retained before final disposal action is taken (i.e. destruction or transfer to our archiving facility).

The document retention schedule applies to information regardless of its format or the media in which it is created or might be held.

3.4.3 Disposal of Documents and Records

All confidential documents and records will be disposed in an appropriate way to ensure the security of that data.

3.5 Mobile and Tracking Devices

3.5.1 Mobile equipment provided to staff and board members have GPS location capability as standard however, the data devices collect will only be used for the reason provided and any data collected, can only be required in line with the reasons below:

- Mobile Phones/PDA's – are provided for employees to communicate with colleagues and customers and for work processes. Mobile Phones/PDA's are enrolled into a mobile device management solution which;
  - Centrally manages employee access whilst protecting data
  - The ability to locate and lock/wipe devices once reported as stolen/missing
  - Ensure compliance with the overall acceptable use policy.

- Laptops – All company issued laptops are installed with a specialist piece of software that;
  - Monitors devices, data, application, and user activity
  - Remediates uncontrolled device risk
  - Lock down rogue devices or at-risk data on unsecured devices
  - Neutralizes threats and prove compliance

- Lone working devices – are provided for the safety of employees during the course of their duties. Users are required to record their planned destinations; the GPS capability will be used to locate and respond in the case of red alert activation or an emergency.

- Vehicle Tracking Device – are fitted to all vehicles in the managed fleet. Further details can be seen in our fleet management guidance and Tracker guidance. This information is used to;
  - improve business performance
  - support business decisions

  As fleet vehicles are not permitted for private use, all data is business related

3.6 CCTV Cameras

Closed Circuit Television cameras are in operation in our offices, flats, schemes, and neighbourhoods for the security of our staff, customers, offices, and assets. It is managed in line with all current relevant legislation.

- Footage is monitored at our control room or at standalone locations across the estates. Access to images is strictly controlled.
- Images are retained for a set period and are then destroyed or overwritten unless needed for the purposes of investigation or when requested by law enforcement.
- Signage is deployed at strategic locations to notify public, visitors, users, and staff that CCTV is in operation and that images are being recorded for the stated purpose.
- An asset register is in place for all Thirteen CCTV cameras
- Operating procedures are in place in all the service areas where cameras are in operation.
- Covert CCTV is used in exceptional circumstances for a defined duration to help to monitor and respond to Anti-Social Behaviour.

3.7 Call Recordings

We hold recordings of your telephone calls to us, as calls to and from our contact centre and Customer Experience teams, and occasionally other teams are recorded for training and monitoring purposes.

Customers that do not wish to be recorded can contact us via email or letter instead.

3.8 Remote/Home Working

- Users must identify themselves to the network by using their own log-on credentials.
- Users must comply with all applicable Thirteen terms and conditions of employment, rules, policies, practices, procedures, work instructions and the reasonable instructions of management. Failure to do so may result in the withdrawal of remote access facilities and possible disciplinary action.
- Each user working remotely is responsible for protecting the integrity of copyrighted software, and following policies, procedures, and practices related to them to the same extent applicable in the conventional workplace.
- Users must deal with all personal information in the same way they would if they were in an office, ensuring they are complying with the GDPR 2018 and DPA 2018.
- Each user must take all precautions necessary to prevent data corruption, for example by use of unauthorised software that may contain a computer virus.
- Ensure that the IT devices being used away from the conventional workplace have appropriate software firewall settings; this is enforced by Thirteen's IT department.
- Though computers connected to Thirteen's office network will be automatically updated, if using home computers, they will need to be manually updated when prompted. It is essential that all users are responsible for updating personal IT devices, which are to be used for work

purposes, because weaknesses in out-dated computer systems could be exploited by cyber criminals.

4 HOW WE MEASURE THE EXPECTATIONS AND OUTCOMES OF THIS FRAMEWORK

Our expectations will be measured by:

4.1 Monitor the number of Data Subject Access requests and data breaches received and the understanding it provides.

4.2 Provide timely updates to Data subject Access requests (DSAR) and data breaches to build confidence and manage expectations and remain compliant with ICO standards.

4.3 Montor and report on compliance where appropriate.

4.4 Ensure all data is collected, processed and stored in line with the most current legislations.

5 CONSIDERATIONS FOR OUR CUSTOMERS AND COLLEGUES.

5.1 We endeavour to understand who our customers are and any specific needs they may with the data we store to underpin our service delivery and ensure our customers are treated fairly and with respect.

5.2 We have effective processes to allow customers and colleagues to request their personal information in place as set out in our supporting documents and further supported by our complaint procedure.

5.3 We consider the expectations of the consumer standards when considering how we communicate; especially with regard to customers' and colleagues' diverse needs and how we inform them in an appropriate way that is clear, accessible, relevant and timely.

5.4 To further consider customers' diverse needs we have made it accessible for customers to contact and engage with us, methods of communication can be seen in the supporting documents.

5.5 We ensure that all customers wanting to influence and scrutinise our strategies, policies and services have equitable opportunities to do this, using a range of different methods and contact styles, to support our customer and their diverse needs.

5.6 We listen and learn from our customers, through feedback and complaints to help inform further service improvements.

5.7 In accordance with their Terms of Reference, the appropriate committee has reviewed and approved this policy to ensure it reflects our service standards and supports customers appropriately

5.8 Review our policies to ensure data is processed appropriately.

6 TRANSPARENCY ARRANGEMENTS ASSOCIATED WITH THIS FRAMEWORK.

We ensure transparency in relation to this policy by:

6.1 Publication of this policy and supporting documentation in all relevant forums and accessible formats

6.2 Publish privacy notices to ensure customers and colleagues know how their data is collected, used, stored and disposed of.

6.3 By responding to any enquires in an appropriate and timely fashion.

7 SUPPORTING DOCUMENTS AND GUIDANCE.

Contents of supporting documentation	
1.	Definitions
2.	7 Principles of GDPR and Rights
3.	Links to: Customer Privacy Notice
4.	How Customers can contact us
5.	Policies Related to this Policy

1. Definitions

The Group – Thirteen Group and any other subsidiary companies.

Data – Information which is being processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded as part of a relevant filing system.
Sensitive/Personal Data - Data that relates to a living individual, which can be identified from the data, includes any expression of opinion about the individual and any indication of the intentions of the data controller in respect of the individual. This includes photographs, email messages and data recorded by CCTV.

Highly Sensitive Data/Special Category Data – Personal data relating to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Genetics
- Physical or mental health or condition
- Sexual life or sexual orientation
- Biometrics (where used for ID purposes)
- Criminal record, any court proceedings or sentence relating to an offence committed or alleged to have been committed.

Data Controller – The person or organisation responsible for the manner in which any personal data is processed. The Group is the data controller; individual members of employees who process data on behalf of the Group are referred to as data users.

Data Processor – Any person/organisation who processes the data on behalf of the Data Controller.

Data Subject – An individual who is the subject of personal data.

Processing – Obtaining, recording or holding the data or carrying out any operation on the data, including organising, adapting or alteration of the data, retrieval, consultation or use of the data.

Relevant filing system – Any set of information relating to individuals relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible.

Board Directors – are those persons who have been elected to act as representatives of Thirteen Group to make decisions on major organisational issues, and who jointly oversee the activities of the business.

Employees – Those persons holding a position within Thirteen Group and have a contract of employment, and those persons undertaking duties on a voluntary basis, i.e. volunteers and board members. For the purpose of this policy, the term also refers to persons employed by organisations contracted to provide services to Thirteen.

Customers – Those persons whose details have been provided to Thirteen either directly or indirectly via a third party for the purposes of Thirteen providing services to those persons, regardless of whether those services have been provided.

Employee Protection Register / Concerns Markers – Is a confidential register which contains details of individuals who have demonstrated violent or abusive behaviour towards staff, board members, volunteers, or agents acting on behalf of Thirteen Group. The Register is a centralised database which is accessible to all staff via Thirteen Group's IT software system.

Social Media – Refers to websites and applications which allow users to create and share content or to participate in social networking.

Cloud Storage System – Is a form of data storage in which digital data is stored in logical pools and spans across several physical servers. The physical servers tend to be owned and managed by hosting companies.

Encryption – Is the process of encoding messages or information in such a way that only authorised parties can read it.

Confidentiality – Is a set of rules which places restrictions on certain types of information.

Confidential Information - Means any non-public information pertaining to Thirteen Group. Confidential information includes information disclosed by Thirteen Group to employees and board members. Confidential information also refers to information

developed by employees and board members during the course of employment with Thirteen Group. This confidential information is regarded as Thirteen Group’s property.

Personal Blog – A website which displays postings by one or more individuals in chronological order, usually accompanied with links to comments on specific postings.

Website – Is a connected group of pages on the World Wide Web regarded as a single entity, usually maintained by one person or organisation and devoted to a single topic or several closely related topics.

Electronic Email - is the exchange of computer-stored messages by telecommunication.

ICT (Information Communication Technology) - is an umbrella term which includes any communication device or application, encompassing but not limited to: radio, television, mobile phones, computer and network hardware and software, satellite systems, tablet devices, as well as the various services and applications associated with them.

Security – Refers to procedures followed, or measures taken to ensure the security of Thirteen Group.

Password / passcode – refers to a string of characters which allows access to a computer, interface, or system.

Electronic Signature – are symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document.

Tracking Device – is an electronic security device which allows the location of an object or person to be monitored.

Social Engineering - refers to psychological manipulation of people into performing actions or divulging confidential information.

Remote Working / Mobile Working - refers to any time spent working from a location other than the normal office base. Remote and mobile working is dependent on technology to connect the employee to the services and networks required to do their job effectively.

Home Working - is when employees and board members regularly undertake work in the home environment, i.e. the personal residence of employees and board directors.

Lone Working - is when an employee or board member performs an activity which is carried out in isolation from other workers without close or direct supervision.

Agile Working – refers to empowering employees to work when, how, and where they choose, to maximise productivity and to deliver the greatest value to the business. However, there is no universal method of agile working.

2. 7 Principles of GDPR and Rights

UK GDPR Principles and Rights

Principles

The General Data Protection Regulation UK 2018 sets out seven key principles:

Principle 1 – lawfulness, fairness and transparency

- Identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data
- Ensure that you do not do anything with the data in breach of any other laws.
- Use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- Be clear, open and honest with people from the start about how you will use their personal data.

Principle 2 – purpose limitation

- Be clear about what your purposes for processing are from the start.
- Record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- Only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

Principle 3 – data minimisation

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Principle 4 – Accuracy

- Take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- Keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- Carefully consider any challenges to the accuracy of personal data.

Principle 5 – storage limitation

- Must not keep personal data for longer than you need it.
- Think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- Have a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- Periodically review the data you hold, and erase or anonymise it when you no longer need it.
- Carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- Keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Principle 6 – Integrity and Confidentiality (security)

- Ensure that you have appropriate security measures in place to protect the personal data you hold.

Principle 7 – Accountability

- The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.
- Have appropriate measures and records in place to be able to demonstrate your compliance.
-

Rights

The UK GDPR sets out eight right for individuals:

The right to be informed

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- Provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’.
- Provide privacy information to individuals at the time you collect their personal data from them.
- Obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.

- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- Regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people but getting it wrong can leave you open to fines and lead to reputational damage.

The right of access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- Cannot charge a fee to deal with a request in most circumstances.

The right to rectification

- The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- Have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the UK GDPR

The right to erasure

- The UK GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- Have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the UK GDPR places an obligation on you to consider whether to delete personal data.

The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- Have one calendar month to respond to a request.

- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

The right to object

- The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- Tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- Have one calendar month to respond to an objection.

Rights related to automated decision making and profiling

- The UK GDPR has provisions on:
    - automated individual decision-making (making a decision solely by automated means without any human involvement); and
    - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The UK GDPR applies to all automated individual decision-making and profiling.
- Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- Only carry out this type of decision-making where the decision is:
    - necessary for the entry into or performance of a contract; or
    - authorised by Union or Member state law applicable to the controller;

or
    - based on the individual's explicit consent.
- Identify whether any of your processing falls under Article 22 and, if so, make sure that you:
    - give individuals information about the processing;
    - introduce simple ways for them to request human intervention or challenge a decision;
    - carry out regular checks to make sure that your systems are working as intended.

3. Useful Links

Privacy & Cookies - Thirteen

4. How customers can contact us

Contact Us - Thirteen

5. Supporting Policies, Framework or Strategies for this Framework

IT Framework

Acceptable use Policy

Safeguarding Adults, young people and children

Fleet management

Customer Privacy Notice

Employee privacy notice (See iTrent – Colleagues Only)

Building Support Control Room – CCTV Procedure

Data Breach procedure

Data protection Impact assessment procedure

Data subject access request procedure

Data Sharing procedure

Data retention schedule