thirteen

Information Governance Framework

April 2022

Lead Manager	Head of Cyber Security and Data Compliance
Date of Final Draft and Version Number	April 2022
Review Date	April 2025
Officer Responsible for Review	Data Compliance Manager (DPO)

Policy Review History

Version number	Changes to Document	Changes Authorised By	Date Approved
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

1 POLICY STATEMENT

1.1 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.

1.2 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 UK General Data Protection Regulation 2018 and the Data Protection Act 2018 to ensure this.

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

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

1.4 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 REFERENCE MATERIAL

2.1 The following information has been used when developing this framework:

- UK General Data Protection Regulation 2018 (GDPR 2018)
- Data Protection Act 2018 (DPA 2018)
- Guidance from the Information Commissioner's Office (ICO) website
- Data Protection Good Practice Guidance
- ICT Security Policy
- CCTV Code of Practice

3 DEFINITIONS

3.1 A full list of definitions is attached at appendix A.

4.1 Data Protection

4.1.1 The UK 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

4.1.2 These principles must be followed by anyone processing personal data. More detailed information regarding the principles is attached at appendix B.

4.1.3 Use of Employee Protection Register / Concerns Markers

Thirteen Group has 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 UK GDPR and DPA 2018.

4.1.4 Data Sharing 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 UK 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 agreement or contract and be bound by the requirements of that agreement.

4.1.5 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.

4.2 Confidentiality

4.2.1 The Group is 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 UK GDPR 2018 and the DPA 2018.

4.2.2 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.

4.2.3 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 UK GDPR 2018 and DPA 2018.

4.2.4 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.

4.2.5 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.

4.2.6 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 UK 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.

4.2.7 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 UK GDPR, or confidential company information has been shared.

4.3 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 UK 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.

4.3.1 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.

4.3.2 Data Subject Access Request

In accordance with the UK 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 by following the Data Subject Access Request Procedure.

4.3.3 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 UK GDPR requires accuracy and one of the rights of the GDPR is the right to rectification which Thirteen 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.

4.3.4 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.

4.3.5 Safeguarding and Prevention of Crime

Thirteen Group is 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.

4.4 Document Management

Thirteen Group will 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.

4.4.1 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.

4.4.2 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.

4.4.3 Disposal of Documents and Records

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

4.5 Mobile and Tracking Devices

Mobile equipment provided to staff and board members have GPS location capability as standard however, the devices will only be used for the reason provided:

- 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 security 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. These are used to;
    - improve business performance
    - support business decisions
    - As fleet vehicles are not permitted for private use

4.6 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.

4.7 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 UK 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.

5 GOVERNANCE INFORMATION

Equality and Diversity	Initial screening indicated no adverse impact on any of the protected characteristics
Environmental Sustainability	TBC
Customer Involvement and Consultation	A brief summary of the findings of all consultation should then be included in this box. *Reviewed by Customer Involvement feedback received and acted on*
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.

6 APPENDICES

- Appendix A – List Of Definitions
- Appendix B – Principles and Rights