

POLICY NUMBER:	DP01	DATE REVIEWED BY BOARD:	November 2025
DEPARTMENT:	Data Protection	DATE OF NEXT REVIEW:	November 2026

1. Policy Scope, Background & Objectives

1.1 Scope

This Data Protection Policy sets out the Squared's commitment and approach to data protection and provides a clear frame of reference for all team members to determine Squared's standards, aims, and ideals in respect of data protection compliance. The policy's objectives are:

- To provide a clear frame of reference for employees to determine Squared's standards, aims, and ideals in respect of data protection compliance;
- To provide information to data subjects, data processors, and the regulatory authorities about how Squared approaches data protection compliance;

Unless otherwise stated this document applies to all **personal data** processed by Squared. It applies to any natural or legal person who process personal data for or on behalf of Squared including: employees, volunteers, casual and temporary employees, directors and officers, external organisations employed as processors and any external organisations or individuals with whom Squared shares or discloses personal data. It also applies where Squared is a joint controller or where relevant, acts as a processor for another controller.

1.2 Background

The processing of personal data in the United Kingdom is regulated by law, principally the United Kingdom General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("The Act"). Other laws inter-relate with the Act and the UK GDPR including but not limited to the Privacy and Electronic Communications Regulations (2003) ("PECR").

The Data Protection Legislation sets out legal responsibilities on all organisations processing personal data and provides for legal rights for the people whose data are being processed. It also sets out the offences, penalties and remedies. Penalties can be imposed on organisations processing personal data including fines of up to £17,500,000 or 4% of prior year global annual turnover (whichever is the greater). There are a number of criminal

offences set out in the Data Protection Legislation and individuals can be held accountable and be sentenced by the courts for offences under the Data Protection Legislation.

This Policy is a public statement describing this Squared's approach to complying with its legal responsibilities in the Data Protection Legislation and how it enables individual rights to be upheld and exercised.

The reader should refer to the Glossary to ensure that they understand the terms used in this Policy.

1.3 Information Governance Framework

The Policy refers to various logs and registers where records are kept that demonstrate the Squared's compliance with the Data Protection Legislation. Responsibility for the security of all documentation and registers contained in the Data Protection toolkit rests exclusively with the Squared. Squared will ensure that they guard against the loss of or corruption of any of the information in their Data Protection Toolkit.

The version control in the footer refers to Squared's version control of this manual.

This manual is a living document and requires periodic review and amendment. It must, at all times reflect the reality of the data protection compliance management arrangements in this Squared.

1.4 Definitions

The terms used in this framework have the meanings attributed to them in the UK GDPR and the Data Protection Act 2018. Principle terms are also defined in the Glossary of this Policy.

2. Policy Statement

Squared is committed to compliance with all relevant Data Protection Legislation. Squared will maintain a suite of policy documents setting out how it intends to implement management controls sufficient to ensure legal compliance with Data Protection Legislation and will ensure that these documents are reviewed periodically to a) test their adequacy in meeting the legal standards as they change over time, and b) to test Squared's compliance with them. Squared will ensure that all relevant personnel and/or other persons it commissions to process personal data on its behalf, either directly or indirectly, have received appropriate and sufficient training in the application of Squared's policies.

The management will ensure that sufficient and appropriate resources are available to ensure that the Squared meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

The management will ensure that Squared works within the 7 data protection principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

Squared will uphold the rights and freedoms of individuals conferred on them by the Data Protection Legislation. Squared will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights.

This policy applies to all of Squared's activities or operations which involve the processing of personal data.

This policy applies to anyone who is engaged to process personal data for or on behalf of Squared including: employees, volunteers, casual and temporary staff, students, directors, board members, and third-parties such as sub-contractors and suppliers, and anyone who Squared shares or discloses personal data with/to.

3. Responsibilities

3.1 Data Controller

Squared is the legal data controller under the Data Protection Legislation.

3.2 The Board of Management.

The board are responsible for the management of Squared and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to Squared being able to operate.

3.3 Management and supervisory staff.

The leadership team in their respective areas of responsibility, must ensure that all team members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Manager must ensure this policy is adhered to.

Line managers and supervisory staff are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

3.4 Data Protection Officer.

Squared shall nominate a Data Protection Officer (DPO) who shall be responsible for maintaining the policies, guidance and training needed to ensure the organisation is compliant with Data Protection Legislation. The DPO shall monitor and report to the senior management in respect of compliance with the manual, arrange for the investigation of any security incidents, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The DPO shall monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into Squared's policy in a change-controlled manner. The DPO will maintain its responsibilities in accordance with section 4.1 of the Data Protection Policy.

3.5 Process Owners

Data processing activities are managed by nominated job roles or individuals. Senior management shall ensure that a process owner is assigned to each data processing activity or business operation. The Process Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned processing activities.

Process Owners are responsible for understanding what personal data is used in their business area and how it is used, who has access to it and why. As a result, they are able to understand and address risks to the data and the organisation.

The DPO shall maintain a list of Process Owners and the data processing activities they are responsible for within the Register of Processing Activities (ROPA).

Process Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR policies and ensuring that all staff are appropriately trained.

3.6 HR Management

Squared shall nominate a person to hold operational responsibility for compliance with data protection compliance in relation to the management of its work force including recruitment and retention. In liaison with the DPO this person is responsible through the staff performance management framework for ensuring that adequate training is provided to all employees to ensure data protection compliance.

The People Excellence & Communications Manager has operational responsibility for compliance with data protection policies and best practice in relation to HR policies and procedures including recruitment and retention.

3.7 IT Management

Squared shall nominate a person to hold operational responsibility for compliance with data protection legislation and best practice for information security. Squared shall document further guidelines for this person in an Information Security Management Policy (ISMP).

3.8 Employees, volunteers, casual/temporary workers, students, directors and board members etc.

Anyone who is directly engaged by the organisation to undertake data processing activities including but not limited to employees, volunteers, casual/temporary workers, students, directors and board members etc. involved in the receipt, handling or communication of

personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact the DPO. Individuals are expected to complete appropriate training annually. Everyone within the Organisation has a duty to respect data subjects' rights to confidentiality.

Disciplinary action could be imposed on team members for non-compliance with relevant policies and legislation.

3.9 Partner & Third-Party Responsibilities

Any Third Party or organisation that is commissioned to process data or receives data from Squared or is able to access any personal data which is within the custody of Squared must enter into a legally enforceable agreement with Squared the nature of which will be determined by the level of involvement with the data that is held/shared/accessed. Any such agreement must be approved by the DPO.

4. Data Protection Policy Detail

4.1 Data Protection Officer (DPO)

Squared have determined that it is required to designate a Data Protection Officer and has documented the rationale underpinning its decision which it shall keep under periodic review. It shall ensure that the DPO's details are recorded on the Register of Fee Payers maintained by the Information Commissioner's Office, and shall ensure that the contact details of the DPO is provided to data subjects and maintained in other relevant documentation. The DPO shall be issued with a job specification formally detailing their key functions and responsibilities.

4.2 Fair Lawful and Transparent processing

The processing of all personal data by Squared will only be undertaken in a fair, lawful and transparent manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data is being collected and to the people who the data is about if personal data is collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the DPO.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful basis for the data processing activities intended to be applied to the personal data. The DPO is responsible for determining the lawful grounds for processing. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented.

Each Process Owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent policy is adhered to and a LIA/PIA is properly undertaken where necessary. The DPO will provide advice regarding lawful processing conditions and maintain a register of the lawful grounds for all of the organisation's processing activities involving the processing of personal data.

Transparency – Squared will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling of personal data. The DPO shall periodically review the apparent transparency.

4.3 Data processing purposes

Personal data shall only be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing shall be undertaken or commissioned without the approval of the DPO who shall maintain a register of data processing activities and their purpose. Process Owners are responsible for ensuring that all of the data processing activities that they

undertake and/or commission have been approved by the DPO. No personal data shall be used for any purpose other than that which it was collected and/or created for without the approval of the DPO.

4.4 Data minimisation

Squared will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that it collects. Process Owners are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data is collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The DPO will provide advice regarding the justification of personal data collected or created.

4.5 Data accuracy

The organisation recognises that the accuracy of data is important and that some data is more important to keep up-to-date than others. The organisation will use its reasonable endeavours to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

Process Owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up-to-date are treated appropriately through erasure or anonymisation. The DPO will provide advice regarding data accuracy.

4.6 Data retention

Squared will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymisation.

Process Owners are responsible for determining the retention period for personal data under their control or sphere of influence and the DPO shall maintain a data retention schedule setting out approved retention periods and end of life treatment. The retention periods for personal data must be approved by the DPO. Because data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and the organisation the DPO will undertake periodic data retention audits.

4.7 Information security

The organisation will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.8 Children's data

Special measures will be taken by the organisation if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests.

4.9 Personal data relating to criminal convictions and offences

If Squared is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

4.10 Special categories of personal data

Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Squared will not process special categories of personal data unless it is necessary. Where the processing of special categories of personal data is necessary, the DPO shall ensure that the lawful grounds for such processing are documented and shall maintain a periodic review of the necessity to processing the special categories of personal data.

4.11 Consent

Squared will interpret consent to be as defined in the GDPR and that any consent shall not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

Squared recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. Squared recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

Where consent is the lawful basis for processing, the DPO shall ensure that consent is properly obtained in accordance with the conditions above.

4.12 Record keeping and accountability

In order to fulfil Squared's responsibility and to be able to demonstrate compliance with Data Protection Legislation as well as in support the policy on transparency the organisation will maintain records of the processing activities that it controls, undertakes or otherwise commissions ("RoPAs") as required by the Data Protection Legislation and specifically those required in Article 30 of the UK GDPR.

The DPO shall be responsible for maintaining the RoPAs and providing them to the Information Commissioner's Office on demand as required.

The organisation shall strive to maintain additional documentation capable of demonstrating accountability as necessary: the DPO shall be responsible for determining what records should be kept, for how long and in what format in order to support its accountability.

4.13 Information rights policy

The organisation recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that the organisation is able to recognise information rights requests and handle them appropriately when they are exercised.

These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data to the organisation and the right escalate the complaint to the ICO and receive judicial remedy and compensation

4.14 Personal Data Breaches policy

The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy.

All team members and individuals with access to personal data for which Squared is either data controller or processor must report all personal data breaches to the DPO as soon as they

become aware of the breach. Squared will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

The DPO shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

4.15 Data Processors

The organisation reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

If Squared wish to appoint a data processor we will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPO shall provide advice and guidance in respect of this.

A written agreement shall be implemented between the organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The DPO shall ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of the Squared without adhering to this policy.

4.16 Data sharing, disclosure and transfer

Squared will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place. Data sharing agreements must be approved by the DPO who will maintain a register of all such agreements. This policy extends to appointing others to process personal data on our behalf, sharing personal data with

organisations, and providing information to ad-hoc requests for information such as those which may be received from the police and other authorities.

The organisation will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the DPO.

The DPO shall implement measures to ensure that this policy is complied with.

4.17 Internationalisation of personal data

Squared will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that Squared undertakes or commissions whether directly or indirectly must be approved by the DPO and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK Government;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has a decision with regard the adequacy of its data protection regime (Adequacy Regulations) issued by the UK Government;
- The transfer is made under the unaltered terms of an International Data Transfer Agreement ("IDTA") issued by the Information Commissioner for such purposes and where required a Transfer Risk Assessment ("TRA") issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

Where necessary the DPO shall ensure that a risk assessment is carried out on any third country the organisation intends to transfer personal data to and that any supplementary measures are implemented as necessary to ensure adequate protection of personal data.

The DPO shall implement measures to ensure that this policy is complied with.

4.18 Risk assessment

Squared will adopt a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. Where necessary it shall, as a minimum, ensure that a

data protection impact assessment is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the DPO.

Squared will maintain a procedure setting out how data protection impact assessments are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs.

The DPO is responsible for maintaining a register of data protection impact assessments that have been undertaken by the organisation and for its periodic review.

4.19 Training and awareness

Squared will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically. DPO shall determine the training needs of those people within their sphere of control and that appropriate data protection awareness and training is provided, measured and reported.

The DPO shall implement measures to ensure that this policy is complied with.

4.20 Continuous Improvement, audit and compliance checking

Squared will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where no-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Board of Directors will be provided with a summary of audit findings periodically.

The DPO will implement measures to ensure that this policy is complied with.

4.21 Data protection by design and by default

Squared shall strive to foster a culture of data protection by design and by default in all of its data processing activities. It shall ensure that measures are in place to encourage all those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities. The organisation shall strive to ensure that by default, only personal data which is necessary for each specific purpose of the processing is processed and that the extent of the processing, period of their storage and their accessibility. In particular, such measures

shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The DPO shall implement measures to ensure that this policy is complied with.

5. Glossary

Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data Subject	any living individual who is the subject of personal data held by an organisation;
Data Process Owner	The person responsible for the instigation or on-going maintenance of a data process or data processing operation;
Personal Data	means any information relating to an identified or identifiable living individual;
Identifiable living individual	means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
Personal identifiable information (PII)	means personal data.
Special Categories of Personal Data	means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Information Incident	means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information;

Information Security Event	an occurrence in a service, system, or network that indicates a possible breach of information security. This includes breaks in policy, failure of controls, or other previously unknown situations;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Risk	The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;
Corporate Data	Corporate data relates to any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures;
Recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
Third-party	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
Third Country	means a territory that is not the United Kingdom in the UK GDPR and means a territory that is not a Member State of the European Union in the EU GDPR;
Profiling	is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual;
Consent	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;

RoPA

means records of processing activities as required by Article 30 of the
GDPR;

Document Control and approval

Issue	Description of Change	Approval	Date of Issue
1.	Initial Issue		22.05.25
2.	DUA Act update	A Bentley & S Mills	10.10.25

