CONTENTS

1. PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR and the Data Protection Act 2018.

2. SCOPE

This policy applies to all employees of Chess ICT Limited and its subsidiaries ("the Chess Group") which includes the brands Chess ICT, Chess Wholesale, Chess Cybersecurity, eBillz and all third parties responsible for the processing of personal data on behalf of the Chess Group.

3. POLICY STATEMENT

The Chess Group is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of the Chess Group people and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to or being processed by the Chess Group.

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. The Chess Group, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose the Chess Group to complaints, regulatory action, fines and/or reputational damage.

The Chess Group leadership team is fully committed to ensuring continued and effective implementation of this policy and expects all Chess Group peolple and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. Governance

3.1.1. Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, the Chess Group has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer reports to the Head of Business Improvement. The Data Protection Officer's duties include:

- Informing and advising the Chess Group and its people who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of the Chess Group's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of the Chess Group's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject access requests;
- Informing senior managers, leaders, and directors of the Chess Group of any potential corporate, civil and criminal penalties which may be levied against the Chess Group and/or its people for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to a Chess Group service/entity
- receives personal data from a Chess Group service/entity
- has access to personal data collected or processed by a Chess Group service/entity.

3.1.2. Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Each Chess Group service/entity "owner" must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Senior Management Team (SMT) for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

3.1.3. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by the Chess Group services/entities owners in relation to this policy, the Data Protection Officer will carry out data protection compliance audits (within the audit programme) for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ✓ Raising awareness.
  - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ✓ Data subject rights.
  - ✓ Personal data transfers.
  - ✓ Personal data incident management.
  - ✓ Personal data complaints handling.
  - ✓ The level of understanding of data protection policies and privacy notices.
  - ✓ The currency of data protection policies and privacy notices.
  - ✓ The accuracy of personal data being stored.
  - ✓ The conformity of data processor activities.
  - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches.

The Data Protection Officer, in cooperation with key business stakeholders from each service/entity owner, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the Chess Group SMT.

3.2. Data Protection Principles

The Chess Group has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, the Chess Group must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the Chess Group must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the Chess Group must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means the Chess Group must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the Chess Group must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality (Security). Personal data shall be 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. The Chess Group must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance. This means the Chess Group must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data Collection

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

3.3.2. Data Subject Consent

Each Chess Group service/entity owner will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, the Chess Group is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3. Data Subject Notification

Each Chess Group service/entity owner will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.4. Data Use

3.4.1. Data Processing

The Chess Group uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of the Chess Group's services/entities.
- To provide services to the Chess Group's stakeholders.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by the Chess Group to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that the Chess Group would then provide their details to third parties for marketing purposes.

Each Chess Group service/entity will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, the Chess Group will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, the Chess Group will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

3.4.2. Special Categories of Data

The Chess Group will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, the Chess Group will adopt additional protection measures.

3.4.3. Children's Data

Children under the age of 13 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

3.4.4. Data Quality

Each Chess Group service/entity will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by the Chess Group to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - ✓ a law prohibits erasure.
    - ✓ erasure would impair legitimate interests of the data subject.
    - ✓ the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.5. Profiling & Automated Decision Making

The Chess Group will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where a Chess Group service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Each Chess Group service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

3.4.6. Digital Marketing

As a general rule the Chess Group will not send promotional or direct marketing material to a Chess Group contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately, and their details should be kept on a suppression list with a record of

their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by the Chess Group for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which the Chess Group services/entities need to retain personal data is set out in the Chess Group's ***'Data Retention Schedule'*** **(Appendix A).** This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6. Data Protection (Security)

Each Chess Group service/entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary.

3.7. Data Subject Rights and Requests

The Data Protection Officer will establish a system/process to enable and facilitate the exercise of data subject rights related to:

- The right to be informed – individuals have the right to be informed about the collection and use of their data. This information is contained within the Chess Group Privacy Policy. The external Privacy Policy relating to clients, customers, suppliers etc can be found on the Chess Group website. The internal Privacy Policy relating to Chess people can be found within the Chess Company Handbook.

- The right of access – individuals are entitled to the following (within one month of request and with no charge):-
    - Confirmation that the Chess Group are processing their data
    - A copy of the personal data held
    - The purposes of the processing
    - The categories of personal data held
    - The recipients or categories of recipient Chess Group disclose the personal data to
    - The retention period for storing the personal data
    - The existence of their right to request rectification
    - The right to lodge a complaint with the ICO
    - Information regarding the source of the data, where it was not obtained directly from the individual
    - The existence of automated decision making, including profiling (if any)
    - the safeguards provided if we transfer personal data to a third country or international organisation

  (the majority of the above are contained within the Chess Group Privacy Policy).

- The right to rectification – individuals have the right to have inaccurate data rectified or completed if incomplete. Chess has one month to respond.

- The right to erasure – also known as the right to be forgotten. Chess has one month to respond. This is not absolute and only applies in certain circumstances. The Data Protection Officer should be consulted in each instance.

- 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, the Chess Group are permitted to store the personal data but not to use it. Chess has one month to respond.

- 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 their own personal data easily from one IT environment to another in a safe and secure way, without effecting its usability.

- The right to object – individuals have the right to object to the processing of their personal data in certain circumstances. The Chess Group may be able to continue processing if we can show we have a compelling reason for doing so. The Data Protection Officer should be consulted in each instance where the Chess Group deem we have a compelling reason to continue to process.

An individual can request to stop processing their personal data for direct marketing at any time. This is an absolute right and there are NO exemptions or grounds to refuse.

- Rights relating to automated decision making including profiling – individuals have the right to receive information regarding any automated decision making that the Chess Group undertake and have the right to request human intervention or challenge an automated decision.

The Chess Group will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. data subjects are entitled to obtain, based upon a request made in writing/email to: compliance@chessict.co.uk .

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in the Chess Group ***'Data Subject Access Rights Policy and Procedure'*** document.

3.8. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention, investigation or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a Chess Group service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any Chess Group service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to a Chess Group contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9. Data Protection Training

All Chess Group people that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, the Compliance Team and each Chess Group service/entity owner will provide regular Data Protection/GDPR training and procedural guidance for their people.

3.10. Data Transfers

Chess Group services/entities may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. The Chess Group services/entities may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject.

3.11. Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer via compliance@chessict.co.uk providing a description of what occurred using the Chess ***"Incident Reporting Form"*** **(Appendix B).** Notification of the incident can be made via e-mail or by speaking with the Data Protection Officer. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the Chess Group SMT, led by the Data Protection Officer will initiate an emergency response team to coordinate and manage the personal data breach response.

3.12.1 Data Breach Reporting Process

In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer via the compliance@chessict.co.uk using the Chess ***Incident Reporting Form.***

It is appreciated that initially details may be limited and a Data Breach not confirmed in the first instance. Section 1 of the form should be completed for ALL incidents with further sections completed dependant of the type of incident and the severity and potential impact. Assistance to complete the form can be sought from the Compliance Team.

The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Officer must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

4. ROLES AND RESPONSIBILITIES

4.1 Implementation

The Chess Group service/entity owners and the SMT must ensure that all Chess Group people responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each Chess Group service/entity owner will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by the Chess Group.

4.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer, or a member of the Quality and Compliance Team via email compliance@chessict.co.uk .

5. REVIEW

This policy will be reviewed by the Data Protection Officer every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

6. RECORDS MANAGEMENT

Chess Group people must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Chess Group recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

7. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. GDPR was accepted law in 2016 and became fully enforceable on the 25th May 2018

Data Protection Act 2018: the Data Protection Act 2018 was passed law on the 25th May 2018. It runs parallel to GDPR and enhances and underlines various pieces of the legislation including the UKs variables and biometrics.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union. Within the UK this is the Information Commissioner's Office.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR/DPA.

Data Subject: a natural person whose personal data is processed by a controller or processor.

Data Breach: a data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. (Not reportable to ICO.)

Data Breach of Personal Identifiable Information: a data breach which includes Personal Identifiable Information of a Data Subject(s). (Reportable to ICO within 72 hours.)

Security Incident: an event that may indicate that the organisation's systems, data or physical enterprise have been compromised or that measures put in place to protect them have failed.

Personal Data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8. RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Data Protection Act 2018

Print Name:	Sandra Lovell-Struthers
Position:	Head of Quality & Compliance /DPO
Signed:	Sandra Lovell-Struthers
Date Created: **Date Reviewed:**	02.03.2018 12.04.2019 17.04.2020

Appendix A

DOCUMENT/DATA RETENTION SCHEDULE

CATEGORY	RETENTION PERIOD
COMPANY & SUPPLIER/CUSTOMER DOCUMENTS	
Formal Company Documents: Statutory books Resolutions	Permanently
Deeds of title Final plans, planning consents, building certifications	Permanently or until six years after property is disposed of
Leases Records of major refurbishments Warranties (building & major refurbishments)	Fifteen years after expiry
Annual Accounts and Annual Review	Permanently
Investment certificates	Permanently
Minutes/Resolutions of Board/Directors Meetings	Permanently
Minutes of general meetings, i.e. general management, departmental, teams	Three years
Contracts with Customers, Suppliers or Agents – All - including: Licensing agreements Indemnities and guarantees	Six years after expiry or termination of the contract
Client Records/Files	Seven years after the last activity
FINANCE DOCUMENTS	
Purchase Invoices & Supplier documentation including: Payments cash book or record of payments made Purchase ledger Invoice – revenue Petty cash records Bank paying in counterfoils Bank statements Remittance advices Bank reconciliations Payroll – All – including salary & tax records, codes, expenses, benefits, pension deductions, overtime records	7 years (6 years plus current year)
Invoice – capital item Receipts cash book Sales ledger	Ten years
Successful quotations for capital expenditure	Permanently
EMPLOYEE/PERSONNEL RECORDS	
Organisational Charts	Permanently
Employee files – All – including: Redundancy details including calculations Life Assurance expression of wish forms	Six years after employment ceases
Accident reports Health & safety records	Three years after the last entry or end of investigation if later
Details of medical schemes	Permanently
Unsuccessful applications for jobs	Six months after notifying the unsuccessful candidate
PENSION RECORDS	
Trust deeds and rules Trustees' minutes Annual accounts Investment and insurance policy records Actuarial reports Contributions	Permanently
Details re current pensioners	Ten years after benefit ceases
Pensions Schemes including: Next of kin/expression of wish forms	Six years after date of death
INSURANCE DOCUMENTS	
Employer's Liability insurance certificates	Forty years
Other Insurance policies	Three years after lapse
Claims correspondence Accident records and relevant correspondence	Three years after settlement
DATA/INCIDENT MANAGEMENT RECORDS	
Subject Access Requests Data Breach Records and Registers Incident Reporting	Five years
OPERATIONAL	
Call Recordings:	.

• Call Recordings specific to customers should be attached to the relevant Customer Client card within the Portal system these would be available for the life of the record • Call Recordings relating to personal incidents or other retained records should be downloaded and attached to the relevant record outside of the calling system • All call recordings within the telephone recording system	• Seven years after the last activity of the record • To be retain for the length of the relevant record • 12 months
OTHER	
Visitor Books/Registers	Three years after the final entry
Emails	Three years within the email system

Appendix B

INFORMATION SECURITY INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED FOR EVERY DATA/INFORMATION SECURITY INCIDENT. COMPLETION IS REQUIRED ASAP AFTER BEING NOTIFIED OF THE INCIDENT/POTENTIAL INCIDENT AS WE ONLY HAVE A 72 HOUR WINDOW TO INFORM THE INFORMATION COMMISSIONERS OFFICE OF A DATA BREACH INVOLVING PERSONAL IDENTIFIABLE INFORMATION.

- **To be completed by the person reporting the incident or the person receiving a verbal report by telephone etc.**
- **The reporting person should liaise with other individuals involved in the incident and where relevant the system and/or information owners.**
- **This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary.**
- **Section 1 should be completed in all instances, depending on the type of incident and the severity of the incident further sections should be completed as necessary.**
- **If any assistance is required, contact a member of the Compliance Team.**
- **Once completed (it is appreciated that dependant on the incident there may be little information available) the form should be attached via a *token* to Compliance – Incident Reporting OR if no access to *Portal* scanned/emailed to compliance@chessict.co.uk and also sandralovellstruthers@chessict.co.uk**
- **Upon receipt Compliance may need to investigate further.**

Confidentiality Notice
Information about actual and suspected information security incidents is confidential and must be shared only with people with designated responsibilities for managing such incidents. Personal data must be shared on a need to know basis; only those people who need this information to deal with the incident and its consequences should know the identity of any individual(s) involved.

1. INCIDENT REPORT	
Date and time of incident	**Location of incident**
How and when did you become aware of the incident?	
Name of person reporting incident	
Name of person/persons also involved or aware of incident	
Contact details; email, telephone	
Brief description of incident and details of the information lost/disclosed/destroyed; asset lost/stolen/damaged, etc	
Brief description of any action taken at the time of the discovery (if any)	
Possible consequences of incident?	

2. ASSESSING THE RISKS AND ACTIONS TO BE TAKEN	
Does the incident need to be reported immediately to the Police?	**YES / NO**
RISK FACTOR	**DETAILS AND ACTION REQUIRED**
Which IT system(s), equipment, devices or building(s) are involved in the security breach?	
What information has been lost or compromised (if any)?	
Are Chess the Data Controller (Owner) of the data?	
How much information has been lost (if any)?	
If the incident involves the loss of a laptop or portable device how recently was the information it held backed up onto central IT systems?	
Does the laptop or device have information stored ONLY on that device. If so how critical is that information to the business?	
Is the incident business critical? Do users rely on access to this particular information asset or can they use other access or manual processes if the information or asset is unavailable?	
Will the loss or compromise of the information have adverse operational, financial, legal, liability or reputational consequences to the business or third parties?	
Is any of the information confidential? Please provide details of any types of information that fall into any of the following categories.	
PERSONAL DATA – If Personal Identifiable Information is involved in ANY format this report MUST be completed and returned ASAP in order to comply with the 72 hour notification to ICO.	
Special Category information (as defined by GDPR & DPA 2018) • Race • Ethnic origin • Politics	

• Religion • Trade union membership • Genetics • Biometrics(where used for ID purposes) • Health • Sex life • Sexual orientation	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas.	
Personal information relating to vulnerable adults and children.	
Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed.	
Security information that may compromise the safety of individuals if disclosed, e.g. addresses, phone numbers.	
Any other personal information that would cause damage or distress to individuals if disclosed without their consent.	
Number of people affected.	
Have all affected individuals been informed?	
Nature of breach (choose most relevant)	• Accidental or unlawful destruction • Loss • Theft • Alteration • Unauthorised disclosure • Unauthorised access to process • Other
OTHER CATEGORIES OF "HIGH RISK" INFORMATION	

Information received in confidence, e.g. legal advice from solicitors, trade secrets, commercially sensitive and other proprietary information received from contractors, suppliers, customers and partners.	
Information that would substantially prejudice the business or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed.	
Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced.	
Information that would compromise the security of buildings, equipment or assets if disclosed.	
Any other relevant information.	
3. WHO ELSE NEEDS TO BE INFORMED	
Reported to the Police?	YES / NO If YES what date: Police Incident Number:
Reported to Data Protection Officer *Token* Compliance – Incident Reporting sandralovellstruthers@chessict.co.uk and compliance@chessict.co.uk	Date:
Reported to other internal stakeholders?	Details: Date:
Major risks escalated to Risk Management Group?	YES / NO If YES what date:
4. FOR DATA PROTECTION OFFICER USE:	
Notification to Information Commissioner's Office.	YES / NO If YES what date:
Notification to Data Subjects.	YES / No If YES what date:

Notification to other external regulator/stakeholder.	YES / NO If YES what date and who:

Sandra Lovell-Struthers

S. Lovell-Struthers
Head of Quality & Compliance