This policy applies to CX Services which trades as CX Services Ltd, and any other Company within the CX Services Ltd Group of Companies. Where reference is made to 'CX Services' or the 'Company' this refers to any of the Companies within the Group.

1. INTRODUCTION

1.1. Introduction

1.1.1. This data protection policy (the "Policy") has been adopted by CX Services in order to set out the principles for protecting data. This policy covers all employees (whether full time or not) and all directors of CX Services, wherever they may be located or working.

1.1.2. This policy covers all the data collected or retained or in the custody or control of CX Services whatever medium data is contained in. This policy is not therefore restricted to information contained in paper documents but includes data contained in an electronically readable format. For the purposes of convenience, in the policy the medium which holds data is called: "a Document".

1.1.3. The data collected or retained or in the custody or control of CX Services can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

1.1.4. Data can also be collected on the behalf of CX Services clients which can include client's customers, suppliers, business contacts, employees, data that has been rented by the Client or on behalf of the Client and other people the organisation has a relationship with or may need to contact.

1.1.5. This policy should be read in conjunction with other policies that have as their objectives the protection and security of data such as the Data Retention Archiving and Destruction Policy and Information Security Policy.

1.1.6. This policy describes how this personal data must be collected, handled and stored to meet the CX Services data protection standards and to comply with the law which include but are not limited to :-

1.1.6.1. the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, and any laws or regulations implementing Directive 95/46/EC (**Data Protection Directive**) or Directive 2002/58/EC (**ePrivacy Directive**); and/or

1.1.6.2. the General Data Protection Regulation (EU) 2016/679 (**GDPR**), and/or any corresponding or equivalent national laws or regulations (**Revised UK DP Law**);

1.2. OBJECTIVES

1.2.1. This data protection policy ensures that CX Services complies with data protection and GDPR laws, protects the rights of staff, customers, clients and partners, is open about how it stores and process individuals' data and protects itself from the risks of a data breach.

1.3 DATA PROTECTION LAWS

1.3.1 The laws detailed in section 1.1.6 describe how organisations including CX Services must collect, handle and store personal information. These rules apply regardless of whether the information is stored electronically, on paper or on other materials.

1.3.2 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

1.3.3 The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1.3.3.1 Be processed fairly and lawfully
1.3.3.2 Be obtained only for specific, lawful purposes
1.3.3.3 Be adequate, relevant and not excessive
1.3.3.4 Be accurate and kept up to date
1.3.3.5 Not be held for any longer than necessary
1.3.3.6 Processed in accordance with the rights of data subjects
1.3.3.7 Be protected in appropriate ways
1.3.3.8 Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

2 Policy Scope

2.1.1. This policy applies to CX Services and any third party suppliers CX Services may use when collecting or retaining or in custody of data.
2.1.2. It applies to all data that CX Services holds relating to identifiable individuals. This can include:
2.1.2.1. Names of individuals
2.1.2.2. Postal address
2.1.2.3. Email address
2.1.2.4. Telephone numbers
2.1.2.5. Transactional data
2.1.2.6. Plus any other information relating to individuals

2.2. DATA PROTECTION RISKS

2.2.1. This policy helps to protect CX Services from some data security risks, including:-
2.2.1.1. **Breaches of confidentiality.** For instance, Information being given out inappropriately.
2.2.1.2. **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
2.2.1.3. **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

2.3. RESPONSIBILITIES

2.3.1. Everyone who works for or with CX Services has some responsibility for ensuring data is collected, stored and handled appropriately.
2.3.2. Each team that handles personal data must ensure that it is handled and processed in line with the policy and data protection principles.
2.3.3. The following people have key areas of responsibility:
2.3.3.1. The **Board of Directors** is ultimately responsible for ensuring that CX Services meets its legal obligations
2.3.3.2. The **Data Officer,** who is currently **Greg Girard** is responsible for:
2.3.3.2.1. Keeping the Board updated about the data protection/GDPR responsibilities, risks and issues.
2.3.3.2.2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
2.3.3.2.3. Arranging data protection training and advice for people covered by this policy.
2.3.3.2.4. Dealing with requests from individuals to see the data CX Services holds about them (also called 'subject access requests')
2.3.3.2.5. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
2.3.3.3. The **Technical Services Managers,** currently **John Lamont and Colin Davidson** are responsible for:
2.3.3.3.1. Ensuring all systems, services and equipment used for storing data meet acceptable security standards
2.3.3.3.2. Preforming regular checks and scans to ensure hardware and software is functioning properly.
2.3.3.3.3. Evaluating any third-party services the company is considering using to store or process data. For instance cloud computing services.
2.3.3.4. The **Sales and Marketing Manager,** currently **Andrew Hore**, is responsible for:
2.3.3.4.1. Approving all data protection statements attached to external communications such as emails and letters.
2.3.3.4.2. Addressing any data protection queries from clients, journalists or media outlets such as websites or newspapers.
2.3.3.4.3. Where necessary, working with other staff to ensure marketing initiatives abide by data protections principles.
2.3.4. General Staff Guidelines include but are not limited to:
2.3.4.1. The only people able to access data covered by this policy should be those who need it for their work.
2.3.4.2. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
2.3.4.3. CX Services will provide training to all employees to help them understand their responsibilities when handling data.
2.3.4.4. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
2.3.4.5. In particular, strong passwords must be used and they should never be shared.
2.3.4.6. Personal data should not be disclosed to unauthorised people, either within the company or externally.
2.3.4.7. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
2.3.4.8. Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

3. DATA STORAGE

3.1. This section describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Director or Data Officer.
3.2. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

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

3.3.1. When not required, the paper or files should be kept in a locked drawer or filing cabinet.

3.3.2. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

3.3.3. Data printouts should be shredded and disposed of securely when no longer required.

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

3.3.5. Data should be protected by strong passwords that are changed regularly and never shared between employees.

3.3.6. If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

3.3.7. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

3.3.8. Servers containing personal data should be sited in a secure location, away from general office space.

3.3.9. Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

3.3.10. Data should never be saved directly to laptops or other mobile devices like tablets or smart phones unless these devices are encrypted as per company policies.

3.3.11. All servers and computers containing data should be protected by approved security software and a firewall.

3.3.12. Data will be permanently deleted at the end of its retention period as detailed in the Data Retention, Archiving and Destruction Policy. Where CX Services is not the Data Controller but the Data Processor, the normal retention period will be three months unless otherwise agreed in writing with the Client or Data Controller. The Client/Data Controller have the option of the data being returned to them prior to destruction.

4. DATA USE

4.1. Personal data is of no value to CX Services unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

4.1.1. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

4.1.2. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

4.1.3. Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

4.1.4. Personal data should never be transferred outside of the European Economic Area.

4.1.5. Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

5. DATA ACCURACY

5.1. The law requires CX Services to take reasonable steps to ensure data is kept accurate and up to date.

5.2. The more important it is that the personal data is accurate, the greater the effort CX Services should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

5.2.1. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

5.2.2. Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

5.2.3. CX Services will make it easy for data subjects to update the information CX Services holds about them. For instance, via the company website.

5.2.4. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

5.2.5. It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

6. SUBJECT ACCESS REQUESTS

6.1. All individuals who are the subject of personal data held by CX Services are entitled to:

6.1.1. Ask what information the company holds about them and why.

6.1.2. Ask how to gain access to it.

6.1.3. Be informed how to keep it up to date.

6.1.4. Be informed how the company is meeting its data protection obligations.

6.1.5. If an individual contacts the company requesting this information, this is called a subject access request.

6.1.6. Subject access requests from individuals should be made by email, addressed to the data controller at info@cxservicesltd.com. The data controller can supply a standard request form, although individuals do not have to use this.

6.1.7. Individuals will not be charged for a subject access request. The data controller will aim to provide the relevant data within 14 days.

6.1.8. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

7. DISCLOSING DATA FOR OTHER REASONS

7.1. In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

7.2. Under these circumstances, CX Services will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

8. PROVIDING INFORMATION

8.1. CX Services aims to ensure that individuals are aware that their data is being processed, and that they understand:

8.1.1. How the data is being used

8.1.2. How to exercise their rights

8.2. To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

9. RELATED POLICES AND DOCUMENTATION

9.1. This policy outlines the general approach taken by CX Services towards the management and storage of personal data and the responsibilities of all CX Services employees must follow to ensure CX Services is compliant with all relevant data legislation.

9.2. There are a number of related polices and other documents that provide full details as to how CX Services manages personal data in line with Data Protections and GDPR legislation. A copy of each of these documents can be found in the policy section of the CX Services Intranet

9.2.1. **Data Privacy Notice**. This relates to data collected, stored, processed and communicated by CX Services for its own needs and aims. It details what data is collected and the basis for this, it details how long data is retained and how CX Services look after the data. A copy of this notice is also available on the Company website.

9.2.2. **Recruitment & Employment Privacy Notice**. This is associated to the Company Data Privacy Notice and details specifically what how personal data is gathered, stored and processed during and after the employee recruitment process and during and after an employee's period of employment with CX Services. This is available on the Company website as well.

9.2.3. **Data Processing Provisions (Client Version)**. This is an agreement put in place between CX Services and each Client where CX Services is acting as a data processor with data owned or the responsibility of the Client. This may be as a standalone agreement or incorporated into a more detailed contract that exists between the Client and CX Services /

9.2.4. **Data Processing Provisions (Agency Version)**. This is an agreement put in place between CX Services and any third party Supplier to CX Services where CX Services supplies personal data, whether its data owned by CX Services or by one of its Clients and defines how CX Services expects the Supplier to act as a data processor while the data is in their possession.

9.2.5. **Data Security Policy**. This policy defines how CX Services keep digital data secure and how digital data is transmitted to and from CX Services

9.2.6. **Security and Staff Confidentiality Policy**. This policy defines the physical security of the CX Services premises to keep both digital and paper data secure and the responsibilities of all employees to with regards to security

9.2.7. **Data Retention, Archiving and Destruction Policy**. This policy defines the path data takes through CX Services from receipt to eventual destruction.

9.2.8. **Data Subject Access Policy**. This policy defines how individuals can request to find out what data is held by CX Services about them, how this information is disclosed and then how subsequent instructions from the individual are enacted.

9.2.9. **Data Breach Policy**. This details what occurs if there has been a data breach and the processes followed by CX Services if and when a breach occurs.