| | |
|---|---|
| | **UNIQWIN UK Ltd** |
| **Title: Data Protection Policy** | **Document Reference: POLICY 025** |
| **Date of Issue: 29.06.2018** | **Next Review Date: 15.09.2021** |

**STATEMENT OF UNQWIN PRIVACY POLICY**

This policy (together with our Conditions of use and any other documents referred to in it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

**Purpose**

The purpose of this Privacy Policy is:

- to assure you that we recognise and fully respect the privacy and personal data of the individuals; and
- to explain what personal information we collect from individuals and how we ensure its best protection.

This Privacy Policy governs Uniqwin UK Limited This Privacy Policy covers only information which is collected by Uniqwin UK Limited.

## 1. Introduction

Uniqwin needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

## 2. Why this policy exists

This Data Protection Policy ensures that Uniqwin:

- Complies with Data Protection Law and follow good practice
- Protect the rights of staff, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

## 3. Data Protection Law

The Data Protection Act 2018 describes how organisations, including Uniqwin, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper, or on other materials. To comply with the Law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is under-pinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection.

## 4. Policy Scope

This policy applies to:

- The head office of Uniqwin
- All staff and volunteers of Uniqwin
- All contractors, suppliers and other people working on behalf of Uniqwin

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- … plus, any other information relating to individuals

## 5. Data Protection Risks

This policy helps to protect Uniqwin from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.

- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.

- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

## 6. Responsibilities

Everyone who works for or with Uniqwin has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Uniqwin meets its legal obligations.

- **The Data Protection Officer** is responsible for:

  - Keeping the Board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Uniqwin holds about them (also called 'Subject Access Requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT Manager** is responsible for:

  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Marketing Manager**, is responsible for:

  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by Data Protection principles.

## 7. General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**

- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.

- Uniqwin **will provide training** to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below. In particular, **strong passwords must be used** and they should never be shared.

- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.

- 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.

- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

## 8. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

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

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

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

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

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

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

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

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

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

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

Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

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

## 9. Data Use

Personal data is of no value to Uniqwin 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:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically.** The IT Manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

## 10. Data Accuracy

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

The more important it is that the personal data is accurate, the greater the effort Uniqwin 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.

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

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

- Uniqwin will make it **easy for data subjects to update the information** Uniqwin holds about them. For instance, via the company website.

- 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.

- It is the Marketing Manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

## 11. Subject Access Requests

All individuals who are the subject of personal data held by Uniqwin UK Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

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

Subject access requests from individuals should be made by email, addressed to the data controller at HR@uniqwin.co.uk The Data Controller will supply a standard request form.

The data controller will aim to provide the relevant data within 30 days.

The data will always verify the identity of anyone making a subject access request before handing over any information. This must be done by asking the applicant for (a) personal identification and (b) address identification.

## 12. Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances Uniqwin UK Ltd 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.

## 13. Disclosure

Uniqwin may share data with other agencies such as the Local Authority, funding bodies and other voluntary agencies.

The Individual will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Uniqwin to disclose data (including sensitive data) without the data subject's consent. These are:

a) Carrying out a legal duty or as authorised by the Secretary of State
b) Protecting vital interests of an Individual
c) The Individual has already made the information public.
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
e) Monitoring for equal opportunities purposes, i.e. race, disability or religion
f) Providing a confidential service where the Individual's consent cannot be obtained or where it is reasonable to proceed without consent, e.g. where we would wish to avoid forcing stressed or ill Individuals to provide consent signatures.

Uniqwin regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

## 14. Providing Information

Uniqwin UK Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. A version of this statement is available on request.

## Glossary of Terms

**Data Controller** The person who (either alone or with others) decides what personal information Uniqwin will hold and how it will be held or used.

**Data Protection Act 1998** The UK legislation that provides a framework for responsible behaviour by those using personal information.

**Data Protection Officer** The person(s) responsible for ensuring that Uniqwin follows its data protection policy and complies with the Data Protection Act 1998.

**Explicit Consent** A freely given, specific and informed agreement by an Individual in the processing of personal information about him/her. Explicit consent is needed for processing sensitive data.

**Individual** The person whose personal information is being held or processed by Uniqwin for example; a client, an employee or supporter.

**Information Commissioner** The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

**Notification** Notifying the Information Commissioner about the data processing activities of Uniqwin as certain activities may be exempt from notification.

**Personal Information** Information about living individuals that enables them to be identified, e.g. name, address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Uniqwin.

**Processing** Means collecting, amending, handling, storing or disclosing personal information.

**Sensitive Data** Refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade Union Membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

**Data Protection Act: Guidance on compliance**

Notes for guidance on the implementation of the Data Protection Act (DPA) 1998

**What does this note cover?**

- It covers the main points in the Data Protection Act which need to be borne in mind in our day to day work.
- Explains what to do if something goes wrong

It is **not** a comprehensive guide to the Act but it does contain links to other sources of information.

**Who needs to read it?**

Anyone who processes personal data and that means almost everyone.

**What is meant by processing?**

The definition of processing is very wide and includes:

- obtaining, recording and holding data;
- performing any operation on the data, including the erasure or destruction of the data.

**What are personal data?**

The Act defines **personal data** as information which relates to a living individual who can be identified:

- from the data or
- from the data **and** other information which is in the possession of, or is likely to come into the possession of, the data controller

The information may be in either electronic or manual (i.e. paper) form.

**Electronic data**

Personal data are caught by the Act if the information is being processed, or is recorded with the intention that it should be processed, 'by means of equipment operating automatically in response to instructions given for that purpose'.

For all practical purposes this means any data held in electronic form.

**Emails**

The Information Commissioner has advised that email messages may be caught by the Act if they identify living individuals and are held, in automated form, in live, archive or back-up systems, or have been deleted from the live system but are still capable of recovery. They may also be caught if, despite having been deleted from the electronic system they are stored in paper form, in relevant filing systems (see next paragraph).

**Manual data (data recorded on paper only)**

The DPA covers all recorded personal data whether this is kept in paper or electronic form. Prior to November 2005 paper data had to be kept as part of 'a relevant filing system' to be within the scope of the DPA. That is no longer the case.

**Terminology used in the DPA**

**Data Controller**

A data controller is:

- a person who alone, jointly or in common with others determines the purposes for which and the manner in which any personal data are processed; and
- responsible for ensuring that the provisions of the Data Protection Act are complied with.

The term 'person' includes legal entities, but everyone who is employed by Uniqwin UK Limited and who processes personal data has a duty to discharge the data controller's responsibilities.

Accountability for information assets rests with the relevant information asset owner (IAO). Each information asset has a designated IAO, who reports to the senior information risk owner (SIRO).

**Data processor**

In some cases external contractors process data on our behalf. These are known as data processors under the Act. But the Department, as the data controller, nevertheless remains responsible for the data processors.

**Data subject**

The data subject is the individual who the personal data is about, i.e. the subject of the data.

**The Data Protection principles**

The Data Protection principles form a central part of the Act and are the 'golden rules' for processing personal data. They must be observed and all staff who process data must be aware of these principles.

The eight principles, together with the conditions for fair and lawful processing mentioned in the first principle, are set out in full on Information Commissioner's Office web site.

In **summary**, however, they require that the data must be:

- fairly and lawfully processed and, in particular, shall not be processed unless certain conditions are met (more stringent conditions apply if the data being processed are classified as "sensitive")
- obtained only for one or more specified and lawful purposes
- adequate, relevant and not excessive to the purpose for which the data are required accurate and, where necessary, kept up-to-date
- kept no longer than necessary

- processed in accordance with the rights of the data subject (which are specified in the Act)
- kept secure against unlawful or unauthorised processing, or accidental loss or erasure
- not transferred to a country outside the European Economic Area (EEA) unless that country ensures an adequate level of protection

The first priority must always be to close or contain the breach and then to mitigate the risks to those individuals that may be affected by it. You should inform the agency data protection officer

**Some other important points to bear in mind when processing personal data**

- When personal data are being obtained, every effort must be made to ensure that the following information is made available to the data subject:
    - the identity of the data controller (see definition of data controller above)
    - the purposes(s) for which the data are to be processed
    - the likely consequences of the processing
    - to whom the data are likely to be disclosed
    - any other information which may be appropriate in the circumstances
- Where personal data are obtained from someone other than the data subject, the foregoing information must be made available to the data subject at the earliest opportunity.
- Persons whose data you are processing must not be misled or deceived as to the purposes for which you are processing their data, or as to whom you may disclose the data.
- Data subjects have a statutory right of access to their data, so whatever you commit to paper or to the computer - including your personal opinions - may have to be retrieved and disclosed to them if a formal enquiry is made.
- Paper and electronic documents must be properly filed, on either registered paper or electronic files. Such files will be subject to disposal agreements which will help to meet the requirement of the Act that personal data must be kept for no longer than necessary.
- The company's rules on security must be observed.

**If something goes wrong?**

If you discover that data has been lost, or if you believe there has been a breach of the data protection principles in the way data is handled, you must immediately inform the relevant information asset owner (IAO) who must follow the Agency policy set out in Agency guidance on reporting unclassified breaches.

as soon as possible.

**How should Data Protection affect the way I organise my work**

- It is even more important that documents, including emails, which contain personal data are:
    - kept in an orderly fashion;
    - filed on registered electronic or paper files as soon as practicable if they are to be retained;
    - Erased or destroyed when they are no longer required.

- You should not keep random collections of odd papers or old emails. If they need to be retained, they should be properly filed, as mentioned above.
- You should observe the company's clear desk policy.
- You should satisfy yourself that, if required, you could retrieve personal data for which you are responsible to answer an enquiry from a data subject.

**Rights of the individual under the DPA**

The most commonly used is the right of an individual to request copies of any personal data being processed about them by the data controller. These requests are known as subject access requests.

In response to a valid request, the individual is entitled to be told:

- whether personal data about them are being processed and, if so, for what purpose(s)
- to whom the data may be disclosed
- the source of the data

The individual, or data subject, is entitled to receive, in an intelligible form, all the information, including email messages where appropriate, which forms the personal data. This may be by way of a transcript, a photocopy or a print-out.

An explanation must be provided if the personal data are held in a form not immediately intelligible to the data subject.

Information which identifies a third party may be withheld unless the individual concerned consents to its disclosure.

**To release or not to release?**

The Act specifies certain circumstances under which personal data can properly be withheld. These are set out in Exemptions from the right of subject access to this guidance.

However, it is the Agency's policy to be as open as possible in response to a subject access enquiry. For example, personal data which are known to exist and are accessible, but which do not necessarily form part of a "relevant filing system" as described in the Act should, as a matter of course, be released unless they are caught by one of the exemptions.

**Other rights**

In addition to subject access rights, the data subject can, in certain circumstances require the data controller to stop processing their personal data or to order the rectification, blocking or erasure of inaccurate data and to claim compensation for damage or distress caused by a breach of the Act.

Where personal data are being processed automatically for the purpose of evaluating matters relating to the data subject, and the processing is likely to constitute the sole basis for a decision affecting the data subject, he/she is entitled to be given an explanation of the logic involved in the decision process.

**What do I do if I receive a request for personal data (a 'subject access enquiry')?**

If you receive a request from a member of the public asking to see their personal data, refer it without delay to Uniqwin's data protection officer (DPO).

Email: HR@uniqwin.co.uk

**How is an enquiry handled?**

The DPO will ensure that it is a valid enquiry. Subject access enquiries are not valid unless they:

- are made in writing by the data subject or his/her legal representative
- contain sufficient information to enable the required information to be located
- we are satisfied that individual requesting the data held on an individual is the same person. (Identity check)

Once the DPO is satisfied that the request is valid, divisions likely to be holding the personal data will be asked to interrogate their systems and to produce the necessary information. The DPO will check that the requirements of the Act have been met and then pass the information to the data subject.

The company must answer a valid request within 30 calendar days of its receipt.

In certain circumstances the data subject has the right to prevent further processing or to order the rectification, blocking or erasure of inaccurate data and to claim compensation for damage or distress caused by a breach of the Act.

**What information must I produce?**

In response to a valid enquiry, the data subject is entitled to be told:

- whether personal data about the individual are being processed and, if so, for what purpose(s)
- to whom the data may be disclosed
- the source of the data

Where personal data are being processed automatically for the purpose of evaluating matters relating to the data subject, and the processing is likely to constitute the sole basis for a decision affecting the data subject, he/she is entitled to be given an explanation of the logic involved in the decision process.

The data subject is also entitled to receive, in an intelligible form, all the information, including email messages where appropriate*, which forms the personal data. This may be by way of a transcript, a photocopy or a print-out. An explanation must be provided if the personal data are held in a form which means they are not immediately intelligible to the data subject. Information which identifies a third party may be withheld unless the individual concerned consents to its disclosure.

(*Note: Advice about subject access to personal data contained in emails can be found on the Information Commissioner's Office web site.)

**Notifying the Information Commissioner**

Notification is the process by which a data controller informs the Information Commissioner about the processing of personal data within the controller's organisation.

The Commissioner uses these details to make an entry in a statutory register which is available to the public for inspection.

Each data controller is allowed only one entry in the register. The entry must be renewed every year.

**Steps to take**

Existing processing activities within Uniqwin should already be covered by the company's notification. The data protection officer (DPO) keeps the notification under review to ensure that it remains accurate and complete.

If a new activity is likely to involve processing personal data, the DPO should be contacted to enquire whether it is covered by the existing notification and, if not, to arrange to have it added.

Managers are responsible for ensuring that the DPO is contacted in accordance with this guidance in relation to possible new notifications or changes to existing notifications.

The DPO also advises on the appropriate form of notification to give to those whose data you will be processing so as to meet the fairness requirements of the First Data Principle.

You can look up the company's notification on the Information Commissioner's Office web site - our notification number is Z6165627. You must not make a direct approach to the Information Commissioner about notification: all such enquiries must be made through the DPO.

**How does Data Protection differ from Freedom of Information?**

The Data Protection Act 1998 relates only to personal data, i.e. data from which living individuals can be identified. The scope of the Freedom of Information Act 2000 is much wider and gives a general right of access to information - other than personal data - held by public authorities.

Information about the impact of FoI contact the company's FoI Officer.

Information about the Act generally, is on the Information Commissioner's Office web site.

More guidance about the implementation of the Freedom of Information Act will be issued in due course.

**Exemptions from the right of subject access**

Personal data held for the following purposes will generally be exempt from the right of subject access and should not therefore be disclosed in response to an enquiry from a data subject.

- National security
- Crime and taxation, including

    - the prevention or detection of crime;
    - the apprehension or prosecution of offenders;
    - the assessment or collection of any tax or duty
- Health, education and social work (this exemption is subject to orders being made by the Home Secretary to bring such exemptions into effect)
- Regulatory activity concerning the protection of members of the public, charities or fair competition in business
  'Special purposes', namely:
    - the purposes of journalism;
    - artistic purposes;
    - literary purposes
- Research, history and statistics
- Information made available to the public under any enactment
- Confidential references given by the data controller
- Judicial appointments and honours
- Crown employment and Crown or Ministerial appointments

If, in response to a subject access enquiry, you are asked to disclose personal data which you think may be covered by one of these exemptions, you should seek advice from the Agency's Data Protection Officer.

Email: HR@uniqwin.co.uk

**Procedure Statements**

Personal data provided by, or about an individual to the company must be processed in accordance with the Act. Data about an individual will only be processed for lawful and fair purposes. The Trust determines the manner and purposes for which personal data may be used. All purposes will be notified to the Information Commissioner.

Personal data about an individual will be processed for various purposes which may include:
a) for all

- facilitate management decisions
- detect fraud
- enable equal opportunities
- address any health and safety issues
- activities under contract;

b) for staff

- assess his/her application to become an employee
- allow the Trust to serve its duties, rights and obligations to the employee, mainly for HR, admin, regulatory or payroll;

c) for customers

- process his/her referral and assess suitability for business relationship
- facilitate the on-going agreement process
- liaise with other partners to facilitate the service
- facilitate research and training

- allow the Company to serve its duties, rights and obligations to customers, principally for admin, regulatory and/or legal purposes;

d) For suppliers

- assess any application for enrolment
- administer suppliers fees and other payments
- administer credit checks or facilitate the certification.
- administer the supplier relationship and accreditation so that the company may properly carry out its duties, rights and obligations.

This list is not exhaustive and merely a guide as there may be other purposes for which personal information can be legally used.