

# KM CARE & SUPPORT SERVICES

## CONFIDENTIALITY & DATA PROTECTION (GDPR) POLICY

**Policy Version:** 1.0

**Effective Date:** August 2026

**Review Date:** August 2027

**Policy Owner:** Business Owner / Manager

**Applies To:** All employees, self-employed workers, bank workers, contractors and anyone acting on behalf of KM Care & Support Services

### 1. Purpose

KM Care & Support Services is committed to protecting the privacy, dignity and confidentiality of every person who uses our services, as well as our staff and workers.

This policy explains how personal information is collected, used, stored, shared and protected in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

Confidential information must only be accessed, used or shared where there is a legitimate and lawful reason to do so.

### 2. Scope

This policy applies to all information handled by KM Care & Support Services, including:

- Client personal information
- Health and care information
- Contact details
- Emergency contact information
- Family and representative information
- Medication information
- Care and support plans
- Risk assessments
- Financial information
- Incident and safeguarding records
- Complaints and feedback

- Staff and worker information
- Photographs, videos and recordings
- Emails, text messages and other electronic communications
- Paper records
- Information stored on phones, computers, tablets or other devices

The policy applies whether information is held electronically, on paper or communicated verbally.

### **3. Confidentiality Principles**

All workers must:

1. Respect the privacy and dignity of clients.
2. Keep personal information confidential.
3. Only access information required for their role.
4. Only share information where there is a lawful and appropriate reason.
5. Avoid discussing clients in public places.
6. Keep paperwork and electronic information secure.
7. Never disclose information to friends, relatives or other clients.
8. Report suspected data breaches immediately.
9. Follow the person's agreed preferences regarding communication and information sharing.
10. Never use confidential information for personal benefit.

Confidentiality continues after a worker leaves KM Care & Support Services.

### **4. What Is Personal Data?**

Personal data is information that can identify an individual, either directly or indirectly.

Examples include:

- Name
- Address
- Telephone number
- Email address
- Date of birth
- Photographs
- Identification numbers
- Care records
- Information about family members
- Financial information
- Information about a person's circumstances

## **Special Category Data**

Some information requires additional protection, including:

- Health information
- Disability information
- Genetic or biometric information where applicable
- Religious or philosophical beliefs
- Sexual orientation
- Racial or ethnic information
- Other information classified as special category data under UK GDPR

Care and support services will commonly handle health and other sensitive information, so workers must take particular care when accessing or sharing it.

## **5. Lawful Processing**

KM Care & Support Services will only process personal information where there is an appropriate lawful basis under UK GDPR.

Depending on the circumstances, this may include:

- Consent
- Performance of a contract
- Legal obligation
- Protection of vital interests
- Public task
- Legitimate interests

Special category information requires an additional lawful condition where applicable.

Workers must not collect or use personal information simply because it may be useful.

Information should be:

- Relevant
- Necessary
- Accurate
- Proportionate
- Up to date
- Used only for appropriate purposes

## **6. Consent**

Where consent is relied upon, it must be:

- Freely given
- Specific
- Informed
- Unambiguous
- Capable of being withdrawn

A person should never feel pressured into providing consent.

Consent may be appropriate for matters such as certain photographs, marketing or particular information-sharing arrangements.

Consent is **not always required** to share information.

For example, information may need to be shared without consent where there is a safeguarding concern, serious risk of harm or another lawful basis for disclosure.

## 7. Confidentiality in Clients' Homes

Workers must maintain confidentiality when working inside a client's home.

Workers must not:

- Discuss one client with another client.
- Discuss a client's personal circumstances with neighbours.
- Discuss clients with friends or relatives.
- Read private documents that are not relevant to their work.
- Access personal correspondence, phones or computers without appropriate permission and a legitimate reason.
- Take photographs of personal documents or information without authorisation.

Workers should be mindful that conversations may be overheard by family members, visitors or neighbours.

## 8. Verbal Confidentiality

Confidential conversations must take place in an appropriate environment.

Workers must not discuss clients:

- In public places
- In shops or cafés
- On public transport

- In communal areas where others may overhear
- On social media
- In personal group chats

Where workers need to discuss a client for legitimate professional purposes, only the minimum necessary information should be shared.

## 9. Information Sharing

KM Care & Support Services recognises that appropriate information sharing can be essential to safe care.

Information may be shared with appropriate professionals or organisations where there is a lawful basis, including where necessary for:

- Safeguarding
- Emergency medical treatment
- Continuity of care
- Preventing serious harm
- Legal obligations
- Managing a person's agreed care and support
- Regulatory requirements

Information should be shared on a **need-to-know basis**.

Workers should not automatically refuse to share information because it is confidential where doing so could place someone at risk.

If unsure, workers must seek advice from the Business Owner/Manager or the appropriate safeguarding/professional authority.

## 10. Safeguarding and Confidentiality

Confidentiality does not prevent safeguarding concerns from being reported.

Where a worker believes that a client or another person may be experiencing abuse, neglect, exploitation or serious harm, the concern must be reported promptly in accordance with the Safeguarding Policy.

Workers must not promise a client that information will be kept secret if the information indicates that someone may be at risk.

The person should be told, where appropriate and safe to do so, that information may need to be shared to protect them or another person.

## **11. Accuracy of Information**

KM Care & Support Services will take reasonable steps to ensure information held is accurate and up to date.

Workers must:

- Record information accurately.
- Avoid assumptions and personal opinions.
- Correct errors appropriately.
- Report important changes in a client's circumstances.
- Never deliberately falsify or alter records.

If an error is discovered, the original record must not be improperly deleted or concealed.

## **12. Data Minimisation**

Only information that is necessary for the service should be collected and retained.

Workers should ask themselves:

“Do I genuinely need this information to carry out my role safely and effectively?”

If the answer is no, the information should not be collected or retained unnecessarily.

## **13. Security of Paper Records**

Paper records must be protected from unauthorised access.

Where applicable:

- Keep records in a secure location.
- Do not leave paperwork unattended in vehicles.
- Do not leave client records visible to visitors.
- Do not take paperwork home unless authorised.
- Dispose of confidential paperwork securely.
- Do not place confidential documents in ordinary household recycling or rubbish.

## **14. Electronic Information**

Electronic information must be protected using appropriate security measures.

Workers must:

- Use strong passwords.
- Keep passwords confidential.
- Lock devices when unattended.
- Keep devices updated.
- Use approved systems where provided.
- Avoid accessing confidential information over unsecured public Wi-Fi where possible.
- Report lost or stolen devices immediately.

Workers must never share passwords with clients, relatives or other unauthorised people.

## **15. Personal Mobile Phones**

Personal mobile phones should not be used to store client information unless this has been specifically authorised and appropriate security measures are in place.

Workers must not:

- Save unnecessary client photographs.
- Screenshot confidential information unnecessarily.
- Store client documents permanently on personal devices.
- Share client information through personal social media.
- Allow family members or friends to access client information.

Where a phone is used for legitimate work communication, workers must take reasonable steps to prevent unauthorised access.

## **16. WhatsApp and Messaging Services**

Where messaging applications are used for work purposes, workers must ensure that only appropriate information is communicated.

Workers must not use group chats to discuss sensitive client information unless the group is authorised for that purpose and appropriate safeguards are in place.

Client information should be kept to the minimum necessary.

Particularly sensitive information should not be communicated through informal messaging unless there is a legitimate reason and appropriate security.

## 17. Photography and Video

Workers must not photograph or record clients without appropriate authorisation.

Photographs must not be taken:

- For personal use
- For social media
- To share with friends or family
- As a curiosity
- Without a legitimate purpose

Where photographs are required for an agreed business purpose, appropriate consent or another lawful basis must be established.

Photographs must be stored securely and deleted when no longer required, subject to applicable retention requirements.

## 18. Social Media

Workers must never post identifiable information about clients on social media.

This includes:

- Names
- Addresses
- Photographs
- Details of illnesses or disabilities
- Details of visits
- Information about family circumstances
- Details of incidents
- Screenshots of messages
- Information that could allow someone to identify the client

Even if a client's name is not mentioned, information may still constitute a breach if the person can be identified.

Workers should also maintain appropriate professional boundaries with clients on social media.

## 19. Email

When sending confidential information by email, workers must:

- Check the recipient carefully.
- Use the minimum necessary information.
- Avoid sending information to the wrong person.
- Use secure/encrypted methods where appropriate.
- Avoid unnecessary sensitive information in subject lines.
- Report accidental disclosure immediately.

A mistaken email containing personal information must be reported as a potential data breach.

## 20. Data Breaches

A data breach may include:

- Sending information to the wrong person
- Losing a phone containing client information
- Losing paperwork
- Unauthorised access to records
- Sharing information with an unauthorised person
- Hacking or malware
- Accidentally posting confidential information online
- Leaving confidential records somewhere they can be accessed
- Disclosing information verbally to someone who should not receive it

### If a breach occurs:

1. Report it to the Business Owner/Manager immediately.
2. Explain exactly what happened.
3. Identify what information may have been disclosed.
4. Identify who may have received or accessed it.
5. Take immediate steps to contain the breach.
6. Do not attempt to conceal the incident.
7. The Business Owner/Manager will assess whether the breach must be reported to the Information Commissioner's Office (ICO) and/or affected individuals.
8. Record the breach and actions taken.

Where a reportable personal data breach is identified, the ICO generally requires notification without undue delay and, where feasible, within **72 hours** of becoming aware of it.

## 21. Data Subject Rights

Individuals have rights under UK data protection law, subject to applicable conditions and exemptions.

These can include the right to:

- Be informed about how their information is used.
- Access their personal information.
- Request correction of inaccurate information.
- Request deletion in certain circumstances.
- Request restriction of processing in certain circumstances.
- Object to certain processing.
- Request data portability in certain circumstances.
- Withdraw consent where consent is the lawful basis.

Any request relating to personal data rights must be passed promptly to the Business Owner/Manager.

Workers must not attempt to deal with formal data protection requests themselves unless authorised.

## **22. Confidentiality After Employment or Engagement Ends**

Workers remain bound by confidentiality after they stop working for KM Care & Support Services.

They must not retain, copy, photograph, download or use client information after their employment or engagement ends unless there is a lawful and authorised reason.

All business records and confidential information must be returned or securely deleted as instructed.

## **23. Third-Party Information**

Workers may encounter information about a client's relatives, neighbours, professionals or other individuals.

This information must also be treated confidentially.

Workers should only record or share third-party information where it is relevant and necessary for the person's care, safety, safeguarding or lawful business purpose.

## **24. Visitors and Family Members**

Family members and representatives may have legitimate involvement in a client's care.

However, workers must not automatically disclose information simply because someone claims to be a relative.

Where necessary, workers should check:

- Who the person is
- Their relationship to the client
- Whether the client has authorised information sharing
- Whether there is a relevant legal authority
- Whether disclosure is otherwise lawful and necessary

Where there is uncertainty, advice must be sought from the Business Owner/Manager.

## **25. Breach of Confidentiality by Staff or Workers**

A deliberate or negligent breach of confidentiality may result in:

- Additional training
- Formal investigation
- Restriction or removal of access to information
- Disciplinary action
- Termination of employment or contract
- Referral to Social Care Wales or another professional/regulatory body where appropriate
- Safeguarding referral
- Police involvement where appropriate

The response will depend on the seriousness and circumstances of the breach.

## **26. Training and Awareness**

All workers must receive appropriate confidentiality and data protection information as part of induction and ongoing training.

Training should cover:

- Confidentiality
- UK GDPR
- Secure record keeping
- Information sharing
- Data breaches
- Social media

- Mobile phone use
- Safeguarding and lawful information sharing

Workers are responsible for asking for clarification if they are unsure about how information should be handled.

## **27. Monitoring and Review**

The Business Owner/Manager will monitor compliance through:

- Record audits
- Supervision
- Incident and breach reviews
- Complaints
- Client feedback
- Training records
- Internal checks
- Policy reviews

This policy will be reviewed at least annually or sooner if there is a significant change in legislation, regulation, guidance, service provision or identified risk.

## **28. Related Policies**

This policy should be read alongside:

- Safeguarding Policy
- Complaints Policy
- Record Keeping Policy
- Consent and Mental Capacity Policy
- Incident Reporting Policy
- Social Media Policy
- Recruitment and Staff Conduct Policy
- Information Sharing Procedure
- Business Continuity Policy

## **29. Policy Statement**

KM Care & Support Services recognises that confidentiality is fundamental to trust.

Every person using our service has the right to expect that their personal information will be treated respectfully, securely and lawfully.

We will collect and use information only where necessary, protect it from inappropriate access or disclosure, and share it responsibly where doing so is necessary to provide safe support or protect people from harm.

**Confidentiality is everyone's responsibility.**

**Policy owner:** Business Owner / Manager

**Version:** 1.0

**Effective:** August 2026

**Review:** August 2027