Data Protection Policy

Responsible director	Shahida Latif-Haider, Executive Director – Transformation and Resources
Policy monitoring body	Strategic Information Group (Review) Group Board (Approval)
Resident input into policy	Customer Experience Committee
Policy review due	April 2029
Linked strategies/policies	ICT, Digital & Data strategy Special Category & Criminal Offence Data policy Information Sharing policy Information Rights policy Information Security policy Data Protection Impact Assessment procedure
Version	V3.3 - EXTERNAL
Date of approval	30 March 2026

1. Purpose and scope

The UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 govern how we store and handle personal data about living individuals. We refer to these laws here as 'the data protection laws'.

These laws are regulated by the Information Commissioner's Office, which we refer to here as 'the Information Commission'.

As a data controller, WCHG must comply with the data protection laws. We are registered with the Information Commission and follow its guidance to protect information rights.

We must also:

- Keep records of our processes and decisions when using personal data
- Respond to regulatory action and pay fines if required.

This policy sets out how we do this. It applies to all colleagues at WCHG. 'Colleagues' means anyone working for us in any capacity, including employees, trainees, interns, agency workers, volunteers, board members, and external committee members.

The term 'colleagues' does not extend to our partners, suppliers and contractors, who have similar responsibilities to look after the personal data we share with them. These responsibilities are set out in our Information Sharing policy.

Colleagues should read this policy alongside:

- The strategies and policies listed on the cover sheet
- Data processing schedules in our contracts with third parties
- Colleague employment contracts and similar agreements
- Any other contractual obligations that govern the way we protect information.

This is not a privacy notice. Our Privacy Notice is available at: wchg.org.uk/privacy-notice.

Customers should read section 6 of this policy to understand how we communicate their information rights.

We have set out our legal duties and key processes in clear language so customers and colleagues can follow them easily. If **colleagues** need help understanding a specific phrase, they can use our Data Protection Glossary. **Customers** can find a short glossary of key phrases at section 10.

2. Policy statement

WCHG will protect the information rights of customers and colleagues. This policy explains how we comply with data protection laws in everyday work.

Compliance means:

- Applying the data protection principles (see section 4) when processing personal information, and having a lawful basis (section 5) to use it
- Respecting individuals' rights under the law (see section 6).

We follow the principle of **privacy by design** (also known as 'data protection by design and default'). We will:

- Take a "privacy first" approach when creating new systems or processes
- Build privacy by design into our strategies, policies, and procedures
- Consider data protection and information rights in papers for Group Leadership Team, and our Board and committees.

3. Roles and responsibilities

To enable WCHG to meet its responsibilities as a data controller, specific individuals or groups have roles which they must carry out to comply with data protection laws. These roles include:

Board:	• Review and approve this policy • Ensure resources and processes enable compliance
Audit & Risk Committee:	• Review the organisation's information risk profile • Review reports from the Data Protection Officer (DPO) and Strategic Information Group • Ask for second- and third-line assurance from internal or external auditors • Report concerns to the Board
Group Leadership Team:	• Ensure compliance with the data protection principles (see section 4) • Recruit and support Data Ambassadors • Include privacy by design in projects • Review reports on high level information risk

Data Protection Officer (or Deputy DPO):	• Monitor and advise on compliance with the data protection laws • Provide training and awareness • Advise on data protection impact assessments • Act as WCHG's contact point with the Information Commission • Investigate data protection complaints and breaches
Information Governance Team:	• Provide advice, guidance, and training • Publish and maintain this policy and ensure privacy notices are available and up to date • Oversee, coordinate and respond to data risk assessments, information rights requests, and information security investigations • Work with ICT, Data & Digital colleagues to conduct data protection and cyber security audits • Support process managers and Data Ambassadors to manage data risks in their processing activities • Highlight high-risk issues to Information Asset Owners/Administrators and escalate at data clinics
Managers and Leaders (including Information Asset Owners/Administrators):	• Make colleagues aware of this policy • Ensure mandatory training is completed • Ensure all processing activities have a valid lawful basis (see section 5) • Manage data processing risks • Complete data protection impact assessments and information sharing agreements for high-risk activities • Request support to create and review privacy statements • Own information assets and update the record of processing activities • Take responsibility for identifying, notifying and supporting information security incidents and rights requests
Data Ambassadors:	• Promote good practice in their teams • Share information across the network • Support transformation projects • Monitor and report on data held in their area

	• Challenge inappropriate data use • Attend network meetings
All Colleagues:	• Complete annual GDPR and cyber awareness training • Use training and support to apply the data protection principles in their work • Follow guidance and tools provided • Report incidents and rights requests • Do not remove or copy personal data when they leave the organisation.

Failure to carry out these responsibilities with an appropriate level of training may amount to misconduct. This will be dealt with under WCHG's disciplinary policy and procedure.

Significant or deliberate breaches of this policy, such as using or sharing customers' personal data without a good reason to do so, may be treated as gross misconduct and could lead to dismissal without notice.

Note: Colleagues who intentionally use personal data for purposes which have not been approved under these roles and responsibilities could be investigated and charged for criminal offences under the data protection laws.

4. The data protection principles

The UK GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles lie at the heart of WCHG's approach to processing personal data.

5. Lawful bases for processing

WCHG must rely on one or more of these lawful bases to process personal data:

- Consent (see below)
- Contract with customers
- Legal obligation
- Vital interests
- Legitimate interests (where these interests outweigh individual rights).
- Recognised legitimate interest (where we need to use this interest for a pre-approved purpose)

For special category data, an additional lawful basis is required. See the Special Category & Criminal Offence Data policy. Always seek advice from the Information Governance team before processing sensitive data.

Consent

When WCHG relies on consent as the lawful basis for processing personal data, we must ensure:

- Consent is freely given, specific, informed, and unambiguous.
- We can demonstrate that consent was obtained.
- Customers are informed about their right to withdraw consent.
- Withdrawal of consent is as easy as giving it and does not affect other rights.
- For children under 13 using online services, consent is obtained from the person with parental responsibility.

The IG team will work with the relevant Information Asset Administrator to stop processing when consent is withdrawn.

Consent may be invalid if these conditions are not met or if there is an imbalance of power. We will usually seek consent only when no other lawful basis applies.

6. Individual rights and fair processing

Individuals have the right to:

- Be informed about how their data is used
- Access their data (known as a Subject Access Request)
- Correct inaccurate data
- Request deletion of data (where appropriate)
- Restrict processing in certain cases
- Receive data in a portable format
- Object to processing, including marketing and profiling.

WCHG protects our customers' information rights by respecting choice and strengthening control. **Colleagues** should read the Information Rights policy to

understand their role in supporting these rights. **Customers** can find out how to exercise these rights on the Information Rights page on our website.

WCHG will provide clear privacy statements wherever data is collected. We will provide customers with specific needs with information in a suitable format to ensure that their consent is informed. The Information Governance team can advise on this.

7. Related policies and guidance

All related information policies listed in the cover sheet are available to **colleagues** on the Information Place. This policy is available for **customers** on our internet.

For advice or help with this policy, **colleagues** should raise a ticket with the Information Governance helpdesk using the "I want to…" option on the intranet. **Customers** can email: informationgovernance@wchg.org.uk

8. Monitoring and review

This policy, and related information policies as required, will be kept under review in case any future changes to the data protection laws have a significant effect on colleague roles and responsibilities.

We will carry out a full review of all our information policies and procedures every three years, by the date shown on the cover sheet.

9. Equality and diversity

WCHG are committed to providing excellent customer services, which are fair, equitable and inclusive. We will make every reasonable effort to ensure that no-one is discriminated against directly or indirectly because of any protected characteristic as defined by the Equality Act 2010 and in line with our reasonable adjustments statement.

We recognise that some protected groups may be disproportionately impacted and will take additional steps in the application of this policy and make reasonable adjustments to ensure compliance with the Act. If you require this policy in a different format, translated, large print, easy read, braille, or an audio copy, contact us by phone on: 0300 111 0000 or by email: inclusionanddiversity@wchg.org.uk

A screening document for this policy has been completed and reviewed by the Equality Impact Assessment (EIA) Panel. Following this review, a full EIA was not found to be necessary.

10. Data Protection Glossary

Phrase	What it means
Data Ambassador	A colleague who works with personal data in their role. They help their team solve data protection issues
Data Breach / Information Security Incident	An information security incident happens when data has been lost, stolen, or misused. The incident is a data breach if the data belong to our customers
Data Protection Act 2018 / UK General Data Protection Regulation	Two UK laws that work together to make sure we use people's information lawfully and fairly. They protect their information rights
Data Protection Impact Assessment	A process we follow when a new project, system or way of working could create a high risk to people's privacy or rights
Data Protection Officer / Deputy Data Protection Officer	Colleagues responsible for making sure we handle personal data legally and safely. Email dataprotection@wchg.org.uk
Information Asset Owner / Administrator	A member of the our Leadership Team who is accountable or responsible for how information is used in their business area
Information Asset Register	A list of all the important information we hold. It shows where it's kept, who is responsible for it, and how it is protected
Information Sharing Agreement	A written agreement we use to share data securely and safely with another organisation
Privacy Notice	A statement that explains to customers and colleagues how their personal data is collected, used and protected
Profiling	Using computerised tools to making predictions about groups of people based on their personal data, to decide how to provide services to them
Records of Processing Activities	A list of all the personal information we use in our processes, and what we do with it
Special Category & Criminal Offence Data	Special Category Data is very sensitive personal Information. It includes details like someone's beliefs, health, sexuality, or biometrics. Criminal offence data covers information about criminal convictions or alleged offences
Subject Access Request	A request made to us under the data protection laws for a copy of an individual's personal data