Confidentiality, Information Governance and Data Protection Policy

Sample policy template. This is a Verivius-authored template anchored to the statutory regulation and current CQC/professional guidance. Tenants must adapt the operational sections to their own organisation, service type, workforce, premises and professional requirements. Where this template and live law or regulator guidance diverge, the live source wins.

Statutory anchor: UK GDPR, the Data Protection Act 2018, and the common law duty of confidentiality. This policy also engages Regulation 17 (good governance), Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936). **Primary source:** https://www.legislation.gov.uk/uksi/2014/2936/regulation/17 **Last reviewed:** 2026-06-10 **Verivius pack version:** v1, 2026-06-10

Policy owner: Registered Manager. Information governance lead: [name / role]. **Applies to:** all staff, workers, agency staff, bank staff, volunteers, contractors, clinicians, managers and anyone who accesses, creates, stores, shares or handles information for the service.

1. What the regulation says

The primary law for this policy is UK GDPR, the Data Protection Act 2018 and the common law duty of confidentiality, which sit outside the CQC Regulations. This policy also engages Regulation 17 (good governance), which requires the secure, accurate and contemporaneous records that information governance protects:

> Systems or processes must be established and operated effectively to ensure compliance with the requirements in this Part. (Reg 17(1): the umbrella duty)
>
> assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services) (Regulation 17(2)(a))
>
> assess, monitor and mitigate the risks relating to the health, safety and welfare of service users and others who may be at risk which arise from the carrying on of the regulated activity (Regulation 17(2)(b))
>
> maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service

> user and of decisions taken in relation to the care and treatment provided. (Reg 17(2)(c): accurate service-user record)
>
> The full text of the regulation is at https://www.legislation.gov.uk/uksi/2014/2936/regulation/17. UK GDPR and the Data Protection Act 2018 are at https://www.legislation.gov.uk/eur/2016/679 and https://www.legislation.gov.uk/ukpga/2018/12. Where this policy and the law or regulation diverge, the law or regulation wins.

2. Plain-English summary

You have to run effective systems and processes to comply with everything else in Part 3. The regulation lists six things those systems must enable in particular: quality assessment and improvement, risk management, accurate service-user records, accurate employment and management records, seeking and acting on feedback, and continually evaluating and improving how you process all this. If CQC requests a written report on quality and risk plus your improvement plans, you have 28 days from the day after the request. Confidentiality and data protection are how a service keeps those records secure, lawful and trusted: personal and confidential information must be handled only for a lawful work reason, kept accurate and secure, shared only where lawful and necessary, and any breach reported and managed straight away.

3. Purpose

The purpose of this policy is to make sure that [Service Name] protects confidential information, manages personal data lawfully, and uses information safely to support care, treatment and governance.

Health and care information is sensitive. Poor information governance can harm people, damage trust, breach confidentiality, compromise safeguarding, disrupt care and create regulatory risk.

This policy supports Regulation 17 good governance, confidentiality duties, UK GDPR, the Data Protection Act 2018, professional standards and the service's duty to maintain secure, accurate and appropriate records.

4. Policy warning

Staff must not access, share, copy, discuss, photograph, remove, disclose or use personal or confidential information unless they have a lawful work reason and are authorised to do so.

Curiosity access is prohibited.

Information must not be shared through personal email, personal messaging apps, personal devices or unauthorised systems unless explicitly approved through service policy and risk assessment.

A confidentiality or data protection breach must be reported immediately.

5. Scope

This policy applies to:

- care records
- clinical records
- appointment records
- referral records
- safeguarding records
- complaint records
- incident records
- staff records
- recruitment records
- training and supervision records
- financial or billing records
- images, photographs, video or audio
- emails and messages
- paper records
- electronic systems
- backups
- mobile devices
- archived records
- information shared with external bodies

It applies to personal data, special category data, confidential information and business-sensitive information.

6. Principles

The service will process personal information according to the following principles:

- lawfully, fairly and transparently
- for specified and legitimate purposes

- limited to what is necessary
- accurate and kept up to date
- kept for no longer than necessary
- protected by appropriate security
- managed with clear accountability

Staff must understand that confidentiality and data protection support safe care; they do not prevent appropriate information sharing where sharing is lawful and necessary.

7. Responsibilities

The provider is responsible for ensuring that data protection and information governance arrangements are in place.

The Registered Manager is responsible for local implementation, breach escalation, staff compliance and governance review.

The information governance lead is responsible for supporting policy, training, audits, privacy information, data sharing and breach management.

All staff are responsible for protecting information, following this policy and reporting concerns immediately.

Contractors and processors must only handle information under approved arrangements.

8. Confidentiality

Staff must keep information confidential unless there is a lawful reason to share it.

Confidential information may include:

- health information
- care and treatment information
- safeguarding information
- family or relationship information
- financial information
- staff information
- complaints and incidents
- appointment or attendance details
- images or recordings
- information about diagnosis, treatment, medication or risk

Staff must not discuss people in public areas, corridors, reception spaces, social settings or online.

9. Access to records

Staff may only access records where they need the information for their role.

Access must be limited to the minimum necessary.

Managers must ensure that system access is:

- role-based
- approved
- reviewed
- removed promptly when no longer needed
- removed when a person leaves
- restricted where concerns arise

Shared logins must not be used unless there is a documented exceptional reason and appropriate controls.

10. Accurate and appropriate records

Records must be accurate, complete, current and relevant.

Staff must not enter information they know to be false or misleading.

Where a record is corrected, the change must be traceable and must not hide the original entry.

Information must be recorded in the correct system or record location.

11. Privacy information

The service must provide clear privacy information explaining how personal information is used.

Privacy information should explain:

- who the provider is
- what information is collected
- why it is used
- lawful basis where required
- who it may be shared with

- how long it is kept
- people's rights
- how to complain
- contact details for information governance queries

Privacy information must be accessible and reviewed when processing changes.

12. Sharing information

Information may be shared where there is a lawful basis and it is necessary.

This may include sharing with:

- GP or treating clinician
- hospital or emergency services
- local authority
- safeguarding authority
- CQC
- police
- coroner
- commissioner
- professional regulator
- pharmacy
- laboratory or diagnostic provider
- insurer or legal adviser where appropriate
- family, representative or advocate where lawful and appropriate

The service must share enough information to support safety and lawful duties, but not more than is necessary.

13. Safeguarding and serious risk

Staff must not use confidentiality as a reason to delay safeguarding action.

Information may need to be shared without consent where this is necessary to protect a child, adult at risk or another person from harm, or where there is another lawful reason.

The reason for sharing without consent must be recorded.

14. Consent and confidentiality

Consent may be relevant to confidentiality and information sharing, but it is not the only lawful basis for using information.

Staff must not promise absolute secrecy.

People should be told, in a way they can understand, when information may need to be shared for safety, safeguarding, legal or regulatory reasons.

15. Communication security

Staff must use approved communication methods.

When sending information, staff must check:

- recipient identity
- email address or contact details
- attachment content
- minimum necessary information
- secure transfer method
- whether encryption or password protection is required
- whether the message should be recorded in the person's record

Emails sent to the wrong person, wrong attachments, lost letters or insecure messages must be reported as potential data breaches.

16. Mobile devices and remote working

Where staff use mobile devices or work remotely, they must:

- use approved devices and systems
- protect passwords
- use multi-factor authentication where required
- avoid public Wi-Fi unless protected by approved controls
- prevent screen visibility by others
- store records only in approved systems
- report loss or theft immediately
- not download records locally unless authorised
- not use personal messaging apps for confidential information unless explicitly approved

Remote working must not reduce confidentiality standards.

17. Paper records

Paper records must be:

- stored securely
- transported safely where necessary
- not left unattended
- not visible to unauthorised people
- returned to secure storage promptly
- disposed of through confidential waste
- tracked where removed from usual storage

Staff must not take paper records home unless authorised.

18. Images, audio and video

Images, audio or video involving people using the service must only be taken where there is a clear lawful reason and proper consent or other lawful basis.

Images must not be stored on personal devices.

The record must explain:

- reason for image or recording
- consent or lawful basis
- where it is stored
- who may access it
- whether it may be shared
- retention period

Intimate or sensitive images require additional controls.

19. Data subject rights

The service must have a process for responding to requests from people about their personal data.

This may include requests to:

- access their data
- correct inaccurate data
- restrict processing
- object to processing
- erase data where applicable

- receive information about how data is used

Requests must be escalated to the Registered Manager or information governance lead immediately.

The service must respond within legal timescales.

20. Data breaches

A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples include:

- lost records
- wrong email recipient
- wrong attachment
- unauthorised access
- stolen laptop or phone
- records left in public area
- cyber incident
- inappropriate social media disclosure
- verbal disclosure to wrong person
- disposal failure

All suspected breaches must be reported immediately and managed under the Data Breach Policy.

21. Retention and disposal

Information must be kept only for as long as required by law, professional guidance, contract, safeguarding need, legal claim risk or service retention schedule.

Records must be disposed of securely when no longer required.

Disposal must be recorded where appropriate.

The service must not keep information indefinitely because it may be useful one day.

22. Processors and third-party systems

Where the service uses external systems or suppliers to process personal data, the provider must ensure there are suitable arrangements in place.

This may include:

- due diligence
- written contract
- data processing agreement
- security assurance
- access controls
- breach notification arrangements
- data location and transfer checks
- exit and deletion arrangements

The service must not upload confidential information to unapproved systems.

23. Training

Staff must receive information governance and confidentiality training during induction and at regular intervals.

Training must include:

- confidentiality
- lawful information sharing
- data protection principles
- secure records
- email and messaging safety
- remote working
- breach reporting
- safeguarding information sharing
- subject access requests
- use of images
- personal device restrictions

Training must be recorded.

24. Audit and governance

The Registered Manager must audit information governance at least annually, and more often where risk requires.

The audit must check:

- privacy information
- staff training
- access controls
- records security
- data sharing records
- breach records
- subject access process
- retention and disposal
- supplier arrangements
- mobile and remote working controls
- action completion

Findings must be added to the action plan or risk register where required.

25. Related policies in this pack

This policy should be read with:

- Data Breach Policy
- Record Keeping and Documentation Standards Policy
- Safeguarding Adults Policy
- Safeguarding Children Policy
- Duty of Candour Policy
- Complaints Policy
- Professional Boundaries and Conduct Policy
- Chaperone Policy
- Consent to Intimate Examinations and Procedures Policy
- Business Continuity and Emergency Preparedness Policy
- Staff Conduct and Disciplinary Policy
- Clinical Photography or Image Policy where used

26. Review

This policy will be reviewed annually, or sooner following a data breach, ICO concern, CQC finding, system change, new supplier, new processing activity, safeguarding concern, change in law or change in national guidance.

27. Sources and further reading

This template is based on CQC's guidance for providers and managers, the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, and other topic-specific legislation and guidance listed below. It is a starting point for adaptation, not a substitute for legal, clinical, HR, safeguarding or specialist professional advice.

- UK GDPR (https://www.legislation.gov.uk/eur/2016/679)
- Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12)
- Common law duty of confidentiality
- ICO UK GDPR guidance
- ICO data sharing code
- NHS Records Management Code of Practice
- NHS Data Security and Protection Toolkit (DSPT), where applicable, including NHS-contracted or DSPT-in-scope services.
- CQC Regulation 17: Good governance
- Human Rights Act 1998 (https://www.legislation.gov.uk/ukpga/1998/42)
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (https://www.legislation.gov.uk/uksi/2014/2936/regulation/17)

28. When to seek further advice

Seek specialist advice where the issue involves serious harm, safeguarding, deprivation of liberty, restraint, children, professional misconduct, controlled drugs, radiation, termination of pregnancy, infection outbreak, water safety, employment dismissal, DBS barring referral, or regulatory enforcement.

29. Document control

Version	Date	Author	Changes
v1	2026-06-10	Verivius (sample)	Initial sample template, conformed to the Verivius policy standard.

This sample policy template was issued by Verivius. It is a template, not a substitute for legal advice or the tenant's own policy-development process. Where this template and live law or regulator guidance diverge, the live source wins.

An example for guidance, not a ready-to-use policy. This sample is deliberately generic and is not a finished policy. Before any service uses it, rewrite it around your own service, procedures, roles and local arrangements, and remove or replace anything you cannot actually provide (for example a reference to specific training you cannot access). It is guidance, not legal advice, and you are responsible for ensuring any policy you adopt is current.