Superior Healthcare Group

# Data Protection Policy

Version 6.0 – June 2026

## Contents

## Version Control

| Document Title | Data Protection Policy |
|---|---|
| **Author** | Jo Rychlik |
| **Last reviewed** | 01/06/2026 |
| **Next review due** | 01/06/2027 |

## Version Details

| Date | Version No | Status | Author | Reviewer | Approved By | Comments |
|---|---|---|---|---|---|---|
| 27/11/2019 | 1.0 | Final | JR | ST | ST | Final for publication |
| 04/12/2020 | 2.0 | Final | JR | ST | ST | Reviewed |
| 03/12/2021 | 3.0 | Final | JR | ST | ST | Reviewed |
| 03/12/2022 | 4.0 | Final | JR | ST | ST | Reviewed |
| 03/12/2023 | 5.0 | Final | JR | ST | ST | Final for publication |
| 25/04/2024 | 5.0 | Final | JR | MP | MP | Reviewed |
| 10/06/2025 | 5.0 | Final | JR | ST | ST | Reviewed (change of DPO from JS Governance to Jo Rychlik) |
| 06/11/2025 | 5.0 | Final | JR | ST | ST | Reviewed (change of job title for Jo Rychlik) |
| 01/05/2026 | 5.1 | Final | JR | ST | ST | Updated to include Data Protection Complaints Process in line with Data (Use and Access) Act 2025 requirements due to come into force on 19 June 2026. |
| 01/06/2026 | 6.0 | Final | JR | ST | ST | Full policy redraft including change of title to Data Protection (from GDPR): updated DBS section, added MFA, password policy, website privacy policy, digital retention, NCSC password guidance. |

## 1. Background

1.1 The Superior Healthcare Group collects and uses personal data about a range of individuals in the course of its business, including current, past and prospective employees, clients, job applicants, website users, and other stakeholders.

1.2 In collecting and using this data, The Superior Healthcare Group is subject to data protection legislation, which sets out how personal data must be handled, protected and deleted.

1.3 This policy sets out The Superior Healthcare Group's approach to data protection, the responsibilities of those who process personal data on the organisation's behalf, and the processes in place to protect the rights of individuals and ensure compliance with the law.

1.4 This policy should be read alongside The Superior Healthcare Group's Privacy Notices, Consent Forms, and Retention Policy.

## 2. Purpose

2.1 To set out The Superior Healthcare Group's obligations under data protection legislation and describe how the organisation meets them.

2.2 To ensure that all individuals who process personal data on behalf of The Superior Healthcare Group understand their responsibilities.

2.3 To define accountability and establish consistent ways of working in relation to the use, storage, retention and security of personal data.

2.4 To provide individuals with a clear route to raise complaints about how their personal data has been handled, and to ensure such complaints are acknowledged, investigated and responded to appropriately.

2.5 To support The Superior Healthcare Group to meet the following CQC Quality Statements:

- WELL-LED: Governance, management and sustainability
- WELL-LED: How people who use the service, the public and employees are engaged and involved

2.6 To meet the legal requirements of the regulated activities The Superior Healthcare Group is registered to provide, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Records Management Code of Practice for Health and Social Care 2016
- Mental Capacity Act 2005

## 3. Scope

3.1 This policy applies to all roles within The Superior Healthcare Group.

3.2 It applies to all individuals whose personal data The Superior Healthcare Group processes, including clients and prospective clients, current and former employees, job applicants, directors, board members, suppliers and third parties with access to Superior Healthcare systems or data.

3.3 Relevant stakeholders include commissioners, family members, advocates, representatives, external health professionals, local authorities and the NHS.

## 4. Definitions

- **UK GDPR:** the UK General Data Protection Regulation, which forms part of UK law and works alongside the Data Protection Act 2018.
- **Data Protection Act 2018:** the UK Act of Parliament that updates and supplements data protection law, sitting alongside the UK GDPR.
- **Data (Use and Access) Act 2025:** legislation that builds on the UK GDPR framework, including strengthened requirements around data subject rights and complaints handling, due to come into force on 19 June 2026.
- **Data Controller:** an organisation that determines the purposes and means of processing personal data. The Superior Healthcare Group acts as a Data Controller in the majority of its processing activities.
- **Data Processor:** an organisation that processes personal data on behalf of a Data Controller.
- **Data Subject:** the individual to whom the personal data relates.
- **Personal Data:** any information relating to an identified or identifiable living person, including names, contact details, photographs, CCTV images and special category data.
- **Special Category Data:** a subset of personal data attracting a higher level of protection. It includes health and medical information, racial or ethnic origin, religious beliefs, sexual orientation, political opinions and biometric data.
- **Processing:** any operation carried out on personal data, including collecting, storing, using, amending, sharing or deleting it.
- **Data Protection Officer (DPO):** the individual responsible for overseeing data protection compliance within The Superior Healthcare Group.

## 5. Data Protection Officer

5.1 The Superior Healthcare Group has appointed a Data Protection Officer (DPO) due to the nature and scale of health data it processes. While not all organisations are legally required to appoint a DPO, The Superior Healthcare Group has done so voluntarily and in line with best practice.

5.2 The DPO is Jo Rychlik, Director of Quality and Governance, and can be contacted at: dpo@superiorhealthcare.co.uk or by telephone on 01227 771133.

5.3 The DPO is responsible for:

- Acting as the main point of contact for data subject rights requests, including Subject Access Requests
- Advising on the correct storage and processing of data in line with current legislation
- Monitoring compliance and advising on any further steps needed
- Overseeing the organisation's Record of Processing Activities (ROPA)
- Responding to data protection complaints and liaising with the Information Commissioner's Office (ICO) where required

## 6. Key Principles

6.1 The UK GDPR sets out six principles that The Superior Healthcare Group must follow when processing personal data. We must also be able to demonstrate compliance with these principles at any time.

- Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner.

- Purpose limitation – data must be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
- Data minimisation – data must be adequate, relevant and limited to what is necessary.
- Accuracy – data must be accurate and kept up to date. Inaccurate data must be corrected or erased without delay.
- Storage limitation – data must not be kept for longer than is necessary for the purposes for which it was collected.
- Integrity and confidentiality – data must be processed securely, protecting against unauthorised access, loss or destruction.

6.2 In addition to complying with these principles, The Superior Healthcare Group adopts a 'privacy by design' approach, meaning data protection is considered from the outset of any new project, system or client engagement rather than as an afterthought.

## 7. Lawful Basis for Processing

7.1 The Superior Healthcare Group only processes personal data where it has a lawful basis to do so. The most commonly relied upon bases are:

- Consent – the data subject has given clear consent to processing for a specific purpose.
- Contract – processing is necessary to perform a contract with the data subject, or to take steps at their request before entering into a contract.
- Legal obligation – processing is necessary to comply with a legal obligation.
- Vital interests – processing is necessary to protect the vital interests of the data subject or another person.
- Public task – processing is necessary to perform a task in the public interest.
- Legitimate interests – processing is necessary for the legitimate interests of The Superior Healthcare Group or a third party, where those interests are not overridden by the rights of the data subject.

7.2 The vast majority of personal data processed by The Superior Healthcare Group is on the basis of contract or legitimate interests. Where consent is relied upon, it must be freely given, specific, informed and unambiguous.

## 8. Special Category Data

8.1 Special category data requires a higher level of protection. The Superior Healthcare Group must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition under Article 9.

8.2 As a health and social care provider, The Superior Healthcare Group processes special category data primarily on the following bases:

- Article 6(1)(e) – processing necessary for the performance of a task carried out in the public interest
- Article 9(2)(h) – processing necessary for the provision of health or social care or treatment, or the management of health or social care systems

8.3 Processing for direct care is carried out under Articles 6(1)(e) and 9(2)(h).

8.4 Processing for non-direct care purposes – such as planning, commissioning or research – will only take place where there is a clear legal basis and, where applicable, in compliance with the National Data Opt-Out.

8.5 Special category data attracts greater regulatory scrutiny. Breaches involving special category data may result in more severe consequences than breaches involving other categories of personal data.

## 9. Rights of Individuals

9.1 Data subjects have the following rights under the UK GDPR. The Superior Healthcare Group has processes in place to respond to each of these within the required timescales.

| Data Subject Right | Timescale | Notes |
|---|---|---|
| Right to be informed | At point of data collection, or within one month if not collected directly from the data subject | |
| Right of access (Subject Access Request) | One month (extendable by two months for complex requests) | |
| Right to rectification | One month | |
| Right to erasure (right to be forgotten) | Without undue delay, no later than one month | Does not apply where legal obligation to retain exists |
| Right to restrict processing | Without undue delay | |
| Right to data portability | One month | Applies to data processed by consent or contract |
| Right to object | On receipt of objection | Absolute right where data used for direct marketing |
| Rights re automated decision making and profiling | Not specified | Must have human review available on request |

9.2 Where a request is manifestly unfounded or excessive, The Superior Healthcare Group may charge a reasonable fee or refuse to act. This decision must be documented and the data subject informed promptly.

## 10. National Data Opt-Out

10.1 The NHS National Data Opt-Out allows individuals to opt out of their confidential patient information being used for research and planning purposes beyond their direct care.

10.2 The Superior Healthcare Group complies with the National Data Opt-Out policy. Where confidential patient information is used or shared for purposes beyond direct care, we will check whether the individual has registered an opt-out and will respect their choice, unless a legal exemption applies.

10.3 This includes:

- Identifying data sharing for planning or research purposes
- Checking opt-out status where applicable, for example via commissioners or NHS data flows
- Respecting opt-outs unless a statutory exemption applies, such as a public health or legal requirement

10.4 Further information and registration is available at: https://www.nhs.uk/your-nhs-data-matters

## 11. Privacy and Fair Processing Notices

11.1 The Superior Healthcare Group is required to inform data subjects about how their personal data is being processed. We do this through Privacy Notices (also referred to as Fair Processing Notices).

11.2 The Superior Healthcare Group produces and maintains at least two Privacy Notices: one for employees and one for clients. These are reviewed and updated regularly.

11.3 Privacy Notices cover personal data obtained other than through the company website. Data collected via the website is governed by the Website Privacy Policy.

11.4 Privacy Notices are made available to data subjects at the point of data collection, or as soon as reasonably practicable thereafter.

11.5 The Superior Healthcare Group also maintains a Website Privacy Policy, which governs the collection and use of personal data obtained through its website, including any contact forms, cookies or tracking technologies. The Website Privacy Policy is published on the organisation's website and is reviewed alongside this policy.

## 12. Consent

12.1 Where consent is the lawful basis for processing, it must be freely given, specific, informed and unambiguous. Consent must be separate from other terms and conditions, and data subjects must be able to withdraw it at any time.

12.2 The Superior Healthcare Group uses template consent forms to obtain consent from clients and, where applicable, employees. Consent forms include additional guidance where the individual is a child or lacks capacity.

12.3 Children: the UK GDPR does not specify a general age of consent for data processing (except for online services, where the age is 13). The Superior Healthcare Group will seek consent from children in a manner that is age-appropriate, using clear and simple language, and will obtain parental or guardian consent where appropriate.

12.4 Individuals lacking capacity: consent will be sought in line with the Mental Capacity Act 2005. Where an individual lacks capacity, The Superior Healthcare Group will identify and work with the appropriate decision-maker.

## 13. Subject Access Requests

13.1 Data subjects have the right to request access to and copies of the personal data The Superior Healthcare Group holds about them (known as a Subject Access Request or SAR). SARs may be submitted in writing by any means. The Superior Healthcare Group will process all SARs in accordance with the following steps.

**Step 1 – Log the request**

- All SARs will be logged, recording the date received, steps taken and the date of the final response. Any failure to respond within the required timescale will also be noted with an explanation.

**Step 2 – Acknowledge receipt**

- The Superior Healthcare Group will acknowledge receipt of the SAR promptly.

**Step 3 – Verify identity**

- We will only respond to a SAR once we are satisfied as to the identity of the applicant. Where we have an existing relationship with the individual, identity will usually be straightforward to confirm. Where we do not recognise the individual or their contact details have changed, we may request proof of identity such as a utility bill or identification document. The one-month response period will commence once identity has been confirmed.

**Step 4 – Clarify scope if needed**

- We may ask the data subject to provide context to help us locate the relevant data, such as relevant dates or the type of document they are seeking. We will not use this to delay our response unless the information is genuinely necessary to locate the data.

**Step 5 – Gather the data**

- We will identify all departments and systems that may hold relevant personal data and collate it in as efficient a manner as possible.

**Step 6 – Consider exemptions**

- We will consider whether any exemptions apply, such as where disclosure would prejudice legal proceedings, reveal the personal data of another individual, or compromise public security. We will seek legal advice where necessary. If a request is manifestly unfounded or excessive, we may charge a reasonable fee or decline the request, with written justification.

**Step 7 – Redact third-party data**

- Where documents contain personal data relating to other individuals, that information will be redacted before disclosure, unless consent has been obtained from the relevant third party.

**Step 8 – Respond**

- The response will include the personal data requested and, if requested, information about the purposes and legal basis for processing, the categories of data held, recipients or categories of recipients, the planned retention period, and information about the data subject's rights.

**Step 9 – Retain a copy**

- A copy of the information provided to the data subject will be retained for 6 months from completion of the request, or until the data subject confirms they require no further information, whichever is sooner.

## 14. Right to Erasure

14.1 Data subjects have the right to request the deletion of personal data held about them in certain circumstances. This is known as the right to erasure or the right to be forgotten.

14.2 On receipt of an erasure request, The Superior Healthcare Group will identify the legal basis for processing the relevant data and determine whether it is required to comply with the request.

14.3 The Superior Healthcare Group is not required to erase data where it has a legal obligation to retain it. For example, records relating to the payment of statutory sick pay must be retained for at least three years following the end of the tax year in which the payment was made.

14.4 Where the lawful basis for processing is legitimate interests, the data must be erased if requested, unless there are compelling grounds for retention that override the data subject's interests, or the data is necessary for the establishment, exercise or defence of legal claims.

14.5 All erasure requests and the decisions made in response to them will be documented.

## 15. Data Breach Notification

15.1 A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

15.2 All employees must immediately report any actual or suspected breach to the Data Protection Officer (DPO).

15.3 The DPO will assess the breach, determine the likelihood and severity of harm, and decide whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required.

15.4 Where notification to the ICO is required, this must be made within 72 hours of The Superior Healthcare Group becoming aware of the breach.

15.5 All breaches, including near misses, will be recorded and reviewed. Where a breach reveals a systemic issue, corrective action and any learning will be documented.

15.6 Examples of breaches include: sending personal data to an incorrect recipient, failure to use BCC when emailing multiple individuals, loss of a device containing personal data, and leaving records accessible to unauthorised individuals.

## 16. Criminal Offence Data and DBS Checks

16.1 As a CQC-regulated provider, The Superior Healthcare Group carries out Disclosure and Barring Service (DBS) checks where it is authorised to do so under legislation. DBS certificate information constitutes special category data under UK GDPR and is handled with the highest level of care.

16.2 The level of check required – standard, enhanced, or enhanced with barred list information – is determined by the nature of the role and the applicable legal framework, including the Rehabilitation of Offenders Act 1974 (Exceptions Order 1975), the Police Act 1997 (Criminal Records) Regulations, and the Safeguarding Vulnerable Groups Act 2006 (as amended by the Protection of Freedoms Act 2012). We will only request a DBS check at the level appropriate to the role and no higher.

16.3 Since 17 June 2013, the DBS sends the certificate to the applicant only. The Superior Healthcare Group does not receive a copy of the certificate. Applicants are required to present their original DBS certificate to an authorised member of staff prior to commencing employment.

16.4 In accordance with CQC's own guidance on DBS checks for social care providers (Registration under the Health and Social Care Act 2008: DBS Checks Guidance v7, October 2019: https://www.cqc.org.uk/sites/default/files/20191113_Disclosure_and_Barring_Service_DBS_checks_guidance_v7.pdf) The Superior Healthcare Group retains the DBS certificate, containing the certificate number, the individual's name, date of issue and level of check until inspectors have seen it or for a maximum of 12 months. This is retained as evidence that a certificate has been obtained.

16.5 Following a CQC inspection, any copies of DBS certificates will be destroyed promptly and securely. While awaiting destruction, certificate information is stored electronically in a secure designated folder within Microsoft Teams, with access strictly limited to authorised individuals.

16.6 Regardless of whether a certificate copy is retained, the following information is recorded permanently on the individual's employment file and retained for the duration of employment and in line with the Retention Schedule:

- The date of issue of the DBS certificate
- The full name and date of birth of the individual
- The type of check requested
- Whether the children's and/or adults' barred list was checked, and the outcome
- The position for which the check was requested
- The unique reference number of the certificate
- The details of the employment decision taken
- Any additional information that may require periodic checks to be made

- Where, following a risk assessment, a decision is taken not to apply for a DBS check, the reason for that decision is recorded on file.

16.7 Where staff are supplied by an employment agency, The Superior Healthcare Group will obtain and retain written confirmation from the agency that a satisfactory DBS check at the appropriate level has been carried out.

## 17. Data Storage and Security

**General principle**

- Personal data must be stored securely, accessed only by those with a legitimate need to do so, and deleted when it is no longer required.

**Database systems**

- The Superior Healthcare Group uses People Planner and Sage Payroll to store the majority of employee and client records. These systems are hosted in secure environments, access is password protected and limited to authorised users, and both systems are maintained in compliance with UK GDPR.

**Network drives and Microsoft Teams**

- Work produced digitally that contains personal data must be stored on the company's shared drives (Microsoft Teams). These are secure, controlled environments that allow data to be located, corrected or removed when required. The DPO has access to these drives for oversight purposes.

**USB sticks and personal devices**

- No employee may use a personal laptop or device for work purposes. USB and SD card ports are locked on most company machines; only authorised senior management machines have active USB ports for essential use. Employees should use shared drives or Teams to share files rather than USB devices.

**Emails**

- Emails sent outside the organisation must not contain personally identifiable data (PID) in the subject line or body of the email. PID must be sent as a password-protected attachment, with the password communicated separately.
- When emailing multiple individuals, all recipient addresses must be placed in the BCC field to prevent recipients from seeing each other's email addresses.
- Emails sent within the organisation should not contain PID in the subject line. Where possible, files should be shared via Teams rather than by email.

**Windows user logins**

- Access to files and systems is controlled via individual Windows login profiles. In line with current National Cyber Security Centre guidance, The Superior Healthcare Group does not require employees to change passwords at regular intervals, as this practice is known to encourage insecure behaviours such as recording passwords or making only minor variations to existing ones. Instead, employees are required to set a strong password at the point of account creation, a minimum of 12 characters using three random words or a passphrase, and to change their password immediately if they suspect it has been compromised or been shared with another person. Accounts are locked after a defined number of unsuccessful login attempts. Where an employee leaves the organisation or changes role, the IT team must be notified promptly so that login access can be removed or updated without delay.

**Multi-Factor Authentication**

- Multi-factor authentication (MFA) is required on all accounts and systems where it is technically available, including Microsoft 365, email, and any system holding personal or sensitive data. MFA provides a second layer of protection

beyond a password, significantly reducing the risk of unauthorised access even where a password has been compromised. Employees must not disable or circumvent MFA on any account. Where a system does not currently support MFA, this should be flagged to the IT team and the DPO so that alternative controls can be put in place and the risk recorded.

## 18.Data Retention

18.1 The Superior Healthcare Group does not retain personal data for longer than is necessary. Retention periods are determined in accordance with legal obligations, NHS Records Management guidance, and the Records Management Code of Practice for Health and Social Care 2016.

18.2 The standard retention periods applied by The Superior Healthcare Group are:

- Employee records (including pay and performance data): 7 years following termination of employment
- Client records (including healthcare information): 20 years following termination of the care arrangement, in line with NHS Records Management requirements
- Unsuccessful recruitment candidates and enquiries: 24 months
- Non-essential emails: cleared regularly; emails older than 1 year should be deleted unless operationally required

18.3 Further detail on retention periods is set out in The Superior Healthcare Group's Retention Policy and Procedure, and the NHS Records Management Code of Practice: https://transform.england.nhs.uk/information-governance/guidance/records-management-code

18.4 Physical records held at Gazette House are reviewed regularly. Records exceeding the relevant retention period are identified and disposed of securely using our external records storage provider (Restore), who provides confirmation certificates of secure destruction. All digital records, including those held on Microsoft Teams, People Planner, Sage Payroll and any other system used by The Superior Healthcare Group, are reviewed and permanently deleted in line with the Retention Schedule.

18.5 Data subjects retain the right to access personal data held about them during the retention period, even after the end of their employment or care arrangement.

## 19. Transfer of Data

19.1 Personal data shared with external organisations is governed by a Data Sharing Agreement (DSA) or Data Processing Agreement (DPA), which sets out the purpose of sharing, the lawful basis, security requirements and the responsibilities of each party.

19.2 Third parties who process personal data on behalf of The Superior Healthcare Group must do so only in accordance with our instructions and in compliance with data protection legislation.

19.3 Where personal data is transferred outside the UK or European Economic Area (EEA), The Superior Healthcare Group will ensure that appropriate safeguards are in place, such as adequacy decisions or Standard Contractual Clauses, and that all legal requirements are met.

## 20. Data Protection Impact Assessments

20.1 A Data Protection Impact Assessment (DPIA) is required where a new or changed processing activity is likely to result in a high risk to individuals. Given The Superior Healthcare Group's routine processing of special category health data, DPIAs are an important part of its governance framework.

20.2 DPIAs are used to identify and mitigate risks before processing begins. They must be completed before any new high-risk processing activity is introduced, including new systems, processes or data sharing arrangements.

20.3 The DPIA process may also be used to review and record data protection incidents, breaches or near misses, and any resulting corrective actions.

20.4 The DPO must be consulted on all DPIAs. Where a DPIA identifies a high residual risk that cannot be mitigated, the ICO must be consulted before processing commences.

## 21. Compliance and Audit

21.1 The Superior Healthcare Group's data protection compliance is overseen by the DPO, Jo Rychlik, Director of Quality and Governance.

21.2 The organisation maintains a Record of Processing Activities (ROPA) setting out the categories of personal data processed, the purposes and legal bases, sharing arrangements and retention periods.

21.3 Compliance is supported through:

- Mandatory annual data security and protection training for all employees, aligned with NHS Data Security and Protection Toolkit (DSPT) requirements
- Clear processes for managing data subject rights requests
- Defined processes for identifying, managing and reporting data breaches
- Regular audits of data processing activities, including annual completion of the NHS DSPT in June each year
- Adherence to retention requirements and secure disposal of records
- Regular review and update of Privacy Notices

21.4 The Superior Healthcare Group aligns its data security practices with the NHS Data Security and Protection Toolkit and the 10 Data Security Standards.

## 22. Data Protection Complaints

22.1The Superior Healthcare Group recognises that individuals have the right to raise a complaint if they have concerns about how their personal data has been handled. Data protection complaints may include concerns about:

- How personal data has been collected, used, shared, stored, retained or deleted
- The handling of a Subject Access Request or other data subject rights request
- The accuracy of personal data held by The Superior Healthcare Group
- The disclosure or redaction of personal data
- Confidentiality concerns or alleged unauthorised access to personal data
- The handling of a personal data breach or suspected breach

**Complaints Process**

22.2 All data protection complaints will be recorded. The Superior Healthcare Group will acknowledge receipt within 5 working days and in any event within 30 calendar days. The DPO, or an authorised member of the Quality and Governance team, will review the complaint and make enquiries without undue delay.

22.3 We will aim to provide a written outcome within 28 calendar days. Where the matter is complex or requires input from multiple teams, the individual will be kept updated and the outcome provided without undue delay.

22.4 Where a complaint identifies a potential data breach, safeguarding concern or legal risk, this will be escalated appropriately and any corrective action or learning recorded.

**How to submit a data protection complaint**

22.5 Data protection complaints should be sent to:

- **Data Protection Officer**, The Superior Healthcare Group Limited, Gazette House, 5-8 Estuary View Business Park, Boorman Way, Whitstable, Kent, CT5 3SE
- **Email:** dpo@superiorhealthcare.co.uk | **Telephone:** 01227 771133

**Escalation to the ICO**

22.6 Individuals are encouraged to raise concerns with The Superior Healthcare Group in the first instance. However, individuals also have the right to complain directly to the Information Commissioner's Office (ICO):

- Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- Website: www.ico.org.uk/concerns

## 23. Further Information and Updates

23.1 This policy and the organisation's Privacy Notices may not cover every aspect of how personal data is collected and used. For further information, please contact the Data Protection Officer using the contact details in Section 22.

23.2 This policy is reviewed annually, or sooner where there are changes to legislation, the organisation's activities, or regulatory requirements. Where changes are made that affect how personal data is used, data subjects will be informed and consent sought where necessary.

23.3 The version number and date of this document will be updated each time it is revised