Remedicare Education Services
Remedicare Privacy Policy (GDPR)
July 2024
Review: July 2025

Remedicare aims to ensure that all personal data collected about staff, students, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1. Introduction - Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

Remedicare does not use formal biometric information.

Remedicare uses CCTV in most communal areas:

Therefore, it also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2. Definitions

Term Definition:

Personal data - Any information relating to an identified, or identifiable, individual.

This may include the individual's:

• Name (including initials)

• Identification number

• Location data

• Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Special categories of personal data Personal data which is more sensitive and so needs more protection, including information about an individual's:

• Racial or ethnic origin

• Political opinions

• Religious or philosophical beliefs

• Trade union membership

• Genetics

• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

• Health – physical or mental

• Sex life or sexual orientation

Processing - Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject - The identified or identifiable individual whose personal data is held or processed.

Data controller - A person or organisation that determines the purposes and the means of processing of personal data.

Data processor - A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. Personal data breach A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Fair Processing Notice - Remedicare has a legitimate interest in processing work email data beyond the point that the employee leaves the company. It is within the lawful basis (section 6, bullet point 4), the purpose of processing being to allow the provision to carry out its official functions, the previous employee's work email will be entered in the DPOs record of processing and will be accessed when needed by the director only, within this Employee Fair Processing Notice. In the event an ex-employee's email is accessed for Remedicare to carry out its functions, Remedicare can't rely on consent for the processing of ex-employee data, the balance of power is wrong, so the consent is not needed or valid.

All employees are informed via the Fair Processing Notice that Remedicare will maintain access to their inbox once they have left.

3. The data controller

Remedicare processes personal data relating to parents, students, staff, directors, visitors and others, and therefore is a data controller. Remedicare is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

4. Roles and responsibilities

This policy applies to all staff employed at Remedicare and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1 Management Committee

The Management has overall responsibility for ensuring that Remedicare complies with all relevant data protection obligations.

4.2 Data protection officer

The data protection officer (DPO) is Dan Nicholson and is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Management and, where relevant, report their advice and recommendations on the Provision's data protection issues. The DPO is also the first point of contact for individuals whose data, the provision processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. **Our DPO is Daniel Nicholson and is contactable via email at Daniel.Nicholson@Remedicare.co.uk**

4.3 Centre Manager

The Centre Manager acts as the representative of the data controller on a day-to-day basis.

4.4 All staff

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the company of any changes to their personal data, such as a change of address

• Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining

personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

The GDPR is based on data protection principles that Remedicare must comply with.

The principles say that personal data must be:

• Processed lawfully, fairly and in a transparent manner

• Collected for specified, explicit and legitimate purposes

• Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is

processed

• Accurate and, where necessary, kept up to date

• Kept for no longer than is necessary for the purposes for which it is processed

• Processed in a way that ensures it is appropriately secure

This policy sets out how the provision aims to comply with these principles.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

• The data needs to be processed so that the provision can fulfil a contract with the individual,

or the individual has asked the provision to take specific steps before entering into a contract

• The data needs to be processed so that the provision can comply with a legal obligation

• The data needs to be processed to ensure the vital interests of the individual e.g. to

protect someone's life

• The data needs to be processed so that the company, as a public authority, can perform a task in the public interest, and carry out its official functions

• The data needs to be processed for the legitimate interests of the company or a third party (provided the individual's rights and freedoms are not overridden.

• The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

6.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data e.g. new intake of students. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs – predominantly for assessment and tracking of learning progress. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the provision's record retention schedule.

7. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

• There is an issue with a student or parent/carer that puts the safety of our staff at risk

• We need to liaise with other agencies – we will seek consent as necessary before doing this

• Our suppliers or contractors need data to enable us to provide services to our staff and student – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are

legally required to do so, including for:

• The prevention or detection of crime and/or fraud

• The apprehension or prosecution of offenders

• The assessment or collection of tax owed to HMRC

• In connection with legal proceedings

• Where the disclosure is required to satisfy our safeguarding obligations

• Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the provision holds about them. This includes:

• Confirmation that their personal data is being processed

• Access to a copy of the data

• The purposes of the data processing

• The categories of personal data concerned

• Who the data has been, or will be, shared with

• How long the data will be stored for, or if this isn't possible, the criteria used to determine

this period

• The source of the data, if not the individual

• Whether any automated decision-making is being applied to their data, and what the

significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO.

They should include:

• Name of individual

• Correspondence address

• Contact number and email address

• Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

8.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or guardian to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardian of pupils at our provision may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardian of students at our provision may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

8.3 Responding to subject access requests

When responding to requests, we:

• May ask the individual to provide 2 forms of identification

• May contact the individual via phone to confirm the request was made

• Will respond without delay and within 1 month of receipt of the request

• Will provide the information free of charge

• May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

• Might cause serious harm to the physical or mental health of the pupil or another individual

• Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

• Is contained in adoption or parental order records

• Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

• Withdraw their consent to processing at any time

• Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

• Prevent use of their personal data for direct marketing

• Challenge processing which has been justified on the basis of public interest

• Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

• Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

• Prevent processing that is likely to cause damage or distress

• Be notified of a data breach in certain circumstances

• Make a complaint to the ICO

• Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances) Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see records

Parents or those with parental responsibility, have a legal right to free access to their child's record (which includes most information about a student) within 15 working days of receipt of a written request.

10. CCTV

At Remedicare we use CCTV in various locations around the provision to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Policy Reviewed July 2024