

Remedicare Education Services

Privacy and Data Protection Policy

Policy Owner: Data Protection Officer

DPO: Daniel Nicholson

DPO Email: Daniel.Nicholson@Remedicare.co.uk

Approved: September 2026

Review Date: September 2027

Applies to: All Remedicare Education Services staff, workers, volunteers, contractors, agency staff and third parties processing information on behalf of Remedicare

1. Purpose and Scope

Remedicare Education Services (“Remedicare”) is committed to protecting the privacy and personal information of the children and young people, parents/carers, staff, volunteers, visitors, commissioners, professionals and other individuals with whom we work.

As an Alternative Provision provider, Remedicare processes personal information as part of delivering education, safeguarding, support, administration, employment and commissioned services.

This policy explains how Remedicare will collect, use, store, share, protect and dispose of personal information.

It applies to personal information held in:

- electronic systems;
- email and messaging systems;
- paper records;
- handwritten notes;
- photographs and videos;
- CCTV;
- safeguarding and incident records;
- education and progress records;
- health and medical information;
- HR and personnel records;
- recruitment records;
- transport and outreach records;
- commissioning and referral records; and
- any other format in which personal information is recorded.

All staff are expected to understand and follow this policy and related procedures.

Failure to comply with data protection requirements may result in management action or disciplinary action, where appropriate.

2. Legislation and Guidance

Remedicare will comply with applicable UK data protection legislation and relevant guidance, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable;
- applicable Equality Act 2010 requirements;
- Information Commissioner's Office (ICO) guidance and codes of practice;
- relevant safeguarding legislation and guidance;
- contractual and commissioning requirements; and
- any other applicable legislation governing the information Remedicare processes.

The Data (Use and Access) Act 2025 has amended aspects of UK data protection law. Remedicare will keep this policy and its associated procedures under review as ICO guidance develops.

Remedicare will also maintain appropriate documentation demonstrating compliance, including, where applicable:

- Records of Processing Activities (ROPA);
- privacy notices;
- data protection impact assessments (DPIAs);
- legitimate interests assessments (LIAs);
- data sharing agreements;
- data processing agreements;
- retention schedules;
- breach records;
- data protection complaints records; and
- records relating to individual rights requests.

3. Key Definitions

Personal data

Personal data is information relating to an identified or identifiable living individual.

This can include:

- name;
- address;
- telephone number;
- email address;
- date of birth;
- identification numbers;
- photographs;
- CCTV footage;
- location information;
- online identifiers;
- education and progress information;
- employment information; and
- information relating to an individual's personal circumstances.

Special category data

Special category data is more sensitive personal information requiring additional protection.

This includes information relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data where used for identification purposes;
- physical or mental health;
- disability;
- sex life; and
- sexual orientation.

Remedicare processes special category information where necessary for purposes such as safeguarding, health and medical support, SEND provision, employment, equality, absence management and other legitimate organisational purposes.

An appropriate Article 9 UK GDPR condition must also be identified where special category data is processed.

Criminal offence data

Information relating to criminal convictions, alleged offences or related proceedings is subject to additional legal requirements.

This may arise in areas such as:

- safer recruitment;
- DBS information;
- safeguarding;
- disciplinary investigations; and
- safeguarding allegations.

Such information must only be accessed and processed where there is an appropriate lawful basis and, where required, an additional condition under data protection law.

Processing

Processing means anything done with personal data, including:

- collecting;
- recording;
- organising;
- storing;
- accessing;
- retrieving;
- using;
- sharing;
- altering;
- transmitting;
- restricting;
- anonymising; or
- deleting.

Data subject

The individual to whom personal data relates.

Data controller

The organisation that determines the purposes and means of processing personal data.

Remedicare is a data controller for the personal data it determines the purposes and means of processing.

Data processor

An organisation or individual that processes personal data on behalf of a data controller.

For example, Remedicare may use external providers for:

- IT systems;
- HR services;
- payroll;
- software platforms;
- cloud storage;
- professional services;
- transport;
- commissioned services; or
- other operational functions.

Where a third party acts as a processor, Remedicare will ensure appropriate contractual and data protection arrangements are in place.

Personal data breach

A personal data breach is a security incident that results in the accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure of; or
- access to

personal data.

Examples include:

- sending information to the wrong person;
- losing a laptop or paper file;
- leaving confidential information unattended;
- sharing information through an inappropriate messaging platform;
- unauthorised access to a system;
- losing a device containing personal information; or
- accidentally publishing personal information.

All suspected data breaches must be reported immediately in accordance with Remedicare's Data Breach Procedure.

4. Remedicare as Data Controller

Remedicare processes personal data relating to:

- children and young people;
- parents and carers;
- staff;
- applicants;
- volunteers;
- directors and managers;
- commissioners;
- local authorities;
- schools and other education providers;
- health and social care professionals;
- visitors;
- contractors;
- suppliers; and
- other individuals involved with Remedicare.

Remedicare will maintain appropriate registration with the ICO where legally required.

5. Data Protection Responsibilities

5.1 Management and Senior Leadership

Remedicare's management and senior leadership are responsible for ensuring that appropriate systems and resources are in place to support compliance with data protection legislation.

This includes ensuring:

- appropriate policies and procedures are maintained;
- staff receive suitable training;
- risks are identified and managed;
- appropriate technical and organisational security measures are used;
- data protection concerns are investigated;
- appropriate contracts and data sharing arrangements are in place; and
- recommendations from the DPO are appropriately considered.

5.2 Data Protection Officer

Remedicare's Data Protection Officer is:

Daniel Nicholson

Email: Daniel.Nicholson@Remedicare.co.uk

The DPO is responsible for overseeing and advising on Remedicare's data protection arrangements.

The DPO will:

- advise Remedicare on data protection obligations;
- monitor compliance with data protection requirements;
- advise on DPIAs and privacy risks;
- advise on data breaches;
- support the handling of individual rights requests;
- support data protection complaints;
- advise on data sharing and data processing arrangements;
- liaise with the ICO where appropriate;
- provide advice and recommendations to senior leadership; and
- support the development and review of data protection policies and procedures.

The DPO should be involved at an early stage where a proposed activity may create significant privacy risks.

The DPO is not personally responsible for ensuring every member of staff complies with data protection law. Responsibility for compliance remains with Remedicare as the data controller and with all staff for the information they handle.

5.3 Managers and Centre Leads

Managers and Centre Leads are responsible for ensuring that staff within their area understand and follow data protection requirements.

They must:

- ensure information is accessed only where required;
- challenge inappropriate handling of personal information;
- report suspected breaches;
- ensure records are stored appropriately;
- support secure information sharing;
- ensure confidential information is not unnecessarily discussed;
- support staff training; and
- escalate concerns to the DPO where appropriate.

5.4 All Staff

All staff are responsible for protecting the personal information they access as part of their role.

Staff must:

- only access information they need for their role;
- only use information for appropriate purposes;
- keep passwords and login information secure;
- lock screens when leaving devices unattended;
- store paper records securely;
- avoid discussing confidential information in public areas;
- use approved Remedicare systems for work information;
- check recipients before sending emails or documents;

- use secure methods when sharing sensitive information;
- report suspected data breaches immediately;
- follow retention and destruction requirements;
- respect individual privacy;
- complete required data protection training; and
- contact the DPO if they are unsure whether information can be accessed, used or shared.

Staff must not:

- access records out of curiosity;
- search for information about a child, parent or colleague without a legitimate work reason;
- photograph confidential documents using a personal device unless specifically authorised;
- store Remedicare personal information on personal devices or accounts unless specifically authorised;
- share passwords;
- send confidential information through personal email accounts;
- discuss confidential information on personal social media;
- leave confidential information unattended; or
- deliberately circumvent Remedicare's security arrangements.

6. Data Protection Principles

Remedicare will comply with the data protection principles.

Personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date where necessary;
5. retained only for as long as necessary;
6. processed securely using appropriate technical and organisational measures; and
7. handled in accordance with the accountability principle.

Remedicare will be able to demonstrate how it complies with these principles.

7. Lawful Processing

Remedicare will only process personal information where an appropriate lawful basis applies.

Depending on the purpose, this may include:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task, where the specific requirements for that basis are met;
- legitimate interests; or
- recognised legitimate interest where the statutory conditions apply.

The lawful basis must be considered for the **specific processing activity** rather than applying one blanket lawful basis to all information processed by Remedicare.

For example, different lawful bases may apply to:

- employment records;
- safeguarding;
- education and progress information;
- health information;
- payroll;
- recruitment;
- CCTV;
- marketing;
- transport;
- commissioning;
- professional information sharing; and
- website use.

Where Remedicare relies upon legitimate interests, it will consider and document the relevant legitimate interests assessment where appropriate.

Remedicare will not use consent simply because it is convenient. Consent must be appropriate for the particular processing activity and must meet the requirements of data protection law.

Where consent is relied upon, individuals must be able to withdraw consent, subject to any other lawful basis that may permit Remedicare to continue processing the information.

8. Children's Personal Information

Remedicare recognises that children and young people require particular care and protection when their personal information is processed.

When processing children's information, Remedicare will consider:

- the child's age;
- their level of understanding;
- their individual circumstances;
- SEND and communication needs;
- whether they can understand the information being provided;
- the nature and sensitivity of the information;
- the purpose of processing; and
- the potential impact on the child.

Privacy information will be presented in a clear and accessible manner appropriate to the intended audience.

Where a child has communication difficulties or additional needs, Remedicare will consider reasonable adjustments to help them understand their data protection rights.

9. Collecting and Using Personal Information

Remedicare will only collect information that is relevant and necessary for the purpose for which it is being collected.

Examples of information processed by Remedicare may include:

Children and young people

- identity and contact information;
- emergency contacts;
- education records;
- EHCP-related information;
- assessment and progress information;
- safeguarding information;

- attendance information;
- behaviour and incident information;
- communication needs;
- health and medical information;
- SEND information;
- transport information;
- family and social information where relevant;
- professional reports; and
- information required to support the commissioned placement.

Parents and carers

- names;
- contact details;
- parental responsibility information;
- communication records;
- relevant family information;
- feedback and complaints;
- consent records; and
- information required to support the child.

Staff and applicants

- identity and contact information;
- employment records;
- recruitment information;
- references;
- DBS and safeguarding information;
- training records;
- attendance and absence information;
- performance information;
- payroll information;
- health information where necessary;
- disciplinary and grievance information; and
- other information required for employment and legal purposes.

10. Data Minimisation

Staff must only collect and use the information necessary for their role.

For example, staff should not routinely copy, download or retain an entire document when only a small amount of information is required.

Where information is no longer required, it must be securely deleted, destroyed or returned in accordance with Remedicare's retention arrangements.

11. Accuracy

Remedicare will take reasonable steps to ensure that personal information is accurate and, where necessary, kept up to date.

Staff should report inaccurate information to the appropriate manager or DPO.

Individuals may also request correction of inaccurate or incomplete information.

12. Information Sharing

Remedicare recognises that appropriate information sharing is an important part of safeguarding and delivering effective Alternative Provision.

Data protection law does not prevent necessary and proportionate safeguarding information sharing.

Personal information may be shared with appropriate organisations where there is a lawful basis to do so.

This may include:

- schools;
- local authorities;
- safeguarding partners;
- children's social care;
- police;
- health professionals;
- SEND services;

- commissioners;
- parents/carers where appropriate;
- emergency services;
- transport providers;
- professional advisers;
- insurers;
- courts or tribunals;
- regulators;
- the ICO; and
- other organisations where legally permitted or required.

Where information is shared, staff must consider:

1. What information is required?
2. Why is it required?
3. Who needs it?
4. What is the lawful basis?
5. Is the information proportionate?
6. Does the recipient have appropriate safeguards?
7. Is there a safeguarding reason requiring information to be shared without delay?

13. Safeguarding Information Sharing

Safeguarding takes priority where there is a risk of harm to a child.

Where information is required to protect a child or another person from harm, staff should not delay necessary information sharing simply because consent has not been obtained.

Staff should seek advice from the DSL and/or DPO where appropriate.

Where there is an immediate safeguarding concern, staff must follow the Child Protection and Safeguarding Policy and contact the appropriate DSL.

Safeguarding information should only be shared with those who need it to safeguard the child or manage the concern.

Staff must not promise absolute confidentiality to children, young people, parents or colleagues.

14. Third-Party Suppliers and Data Processors

Where Remedicare uses a third party to process personal data on its behalf, appropriate due diligence and contractual arrangements will be undertaken.

Where required, a Data Processing Agreement or appropriate contractual provisions will be used.

Remedicare will consider:

- the purpose of processing;
- the categories of information;
- security arrangements;
- confidentiality;
- sub-processors;
- data retention;
- deletion or return of information;
- data breach arrangements;
- international transfers; and
- individual rights.

Only information necessary for the service should be shared.

15. International Data Transfers

Where personal data is transferred outside the UK, Remedicare will ensure that the transfer complies with applicable UK data protection requirements.

Appropriate safeguards will be considered before personal data is transferred internationally.

Staff must not use an overseas service or application to process Remedicare personal information without appropriate approval.

16. Data Security

Remedicare will use appropriate technical and organisational measures to protect personal information.

This may include:

- password protection;
- access controls;
- role-based permissions;
- secure cloud systems;
- encryption where appropriate;
- locked storage;
- secure disposal;
- staff training;
- confidentiality requirements;
- antivirus and security controls;
- device management;
- secure email arrangements;
- restricted access to safeguarding information; and
- regular review of information security arrangements.

Access to information should be based on a genuine need to know.

17. Email and Electronic Communication

Staff must take care when sending personal information by email.

Before sending an email containing personal or sensitive information, staff should check:

- the recipient's email address;
- whether the recipient is authorised to receive the information;
- whether all attachments are appropriate;
- whether the information should be encrypted or otherwise secured;
- whether only the minimum necessary information has been included.

Where an email has been sent to the wrong recipient, staff must report the incident immediately as a potential data breach.

18. Personal Devices and Messaging Applications

Remedicare personal information should not normally be stored on personal devices.

Staff must not use personal email accounts or personal cloud storage to store Remedicare information unless specifically authorised.

Where an approved messaging application is used for operational communication, staff must follow Remedicare's rules regarding:

- confidentiality;
- appropriate content;
- safeguarding;
- retention;
- deletion;
- access;
- screenshots;
- photographs; and
- personal information.

Staff must not share confidential information through personal social media.

19. Photographs and Videos

Photographs and videos may constitute personal data.

Where Remedicare takes photographs or videos, it will consider:

- the purpose;
- the lawful basis;
- whether consent is required;
- the individual's reasonable expectations;
- how the image will be used;
- where it will be stored;
- who will have access; and
- how long it will be retained.

Staff must only take photographs using approved devices and systems where required for their role.

Photographs or videos of children must not be taken on personal devices unless there is an exceptional and authorised reason.

20. CCTV

Remedicare may use CCTV at its premises and other locations where appropriate for purposes including:

- safeguarding;
- health and safety;
- security;
- prevention and detection of crime;
- protection of children, staff and visitors;
- investigation of incidents; and
- protection of Remedicare property.

CCTV will only be used for appropriate and proportionate purposes.

CCTV signs will be displayed where required so that individuals are aware that recording is taking place.

Remedicare will maintain appropriate information about its CCTV processing, including its purpose, lawful basis, retention arrangements and access arrangements.

CCTV footage will only be accessed by authorised individuals with a legitimate reason.

Requests for CCTV footage should be referred to the DPO.

Remedicare will not use biometric identification systems unless separately assessed, approved and implemented in accordance with applicable data protection requirements.

21. Employee Email Accounts After Employment Ends

Remedicare may need to retain or access information contained within an employee's work account after employment ends where there is a legitimate and necessary business, legal, safeguarding, regulatory or operational reason.

This is **not based on employee consent**.

Access will be proportionate and limited to the information required for the relevant purpose.

Where practicable:

- access will be restricted to authorised individuals;
- the account will not be routinely monitored without a legitimate reason;

- access will be documented where appropriate;
- personal correspondence will not be accessed unnecessarily; and
- information will be retained only for as long as necessary.

The existence of an ongoing need to retain or access work information does not mean that Remedicare will retain unrestricted access to an individual's mailbox indefinitely.

Remedicare will manage former employee accounts in accordance with its retention and information security arrangements.

22. Data Retention

Remedicare will not retain personal information for longer than necessary.

Retention periods will be determined by:

- legal requirements;
- safeguarding requirements;
- contractual requirements;
- commissioning requirements;
- operational need;
- regulatory expectations;
- potential legal claims; and
- the nature and sensitivity of the information.

Remedicare will maintain a Records Retention Schedule identifying appropriate retention periods.

When information is no longer required, it will be securely deleted, destroyed or anonymised.

Information subject to an investigation, safeguarding concern, legal claim or other legitimate reason for continued retention may need to be retained beyond the normal period.

23. Personal Data Breaches

All staff must report a suspected personal data breach immediately to their manager and/or DPO.

Examples include:

- sending an email to the wrong person;
- losing a laptop;
- losing a paper file;
- accidentally sharing a safeguarding document;
- leaving confidential information in a public area;
- unauthorised access to a system;
- accidental disclosure of a child's information;
- lost or stolen device; or
- inappropriate access to records.

Staff should **not delay reporting because they are unsure whether the incident constitutes a breach**.

Remedicare will assess the incident and determine:

- what information was involved;
- whose information was affected;
- the potential impact;
- whether containment is required;
- whether individuals need to be informed;
- whether the ICO must be notified; and
- whether further safeguarding or management action is required.

Where legally required, the ICO will be notified within the applicable statutory timeframe.

All significant breaches will be recorded in accordance with the Data Breach Procedure.

24. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be considered where proposed processing is likely to result in a high risk to individuals' rights and freedoms.

Examples may include:

- new technology;
- significant monitoring;
- large-scale processing of sensitive information;
- biometric technology;
- new CCTV or surveillance systems;
- artificial intelligence systems;

- significant changes to children's information processing; or
- other high-risk processing.

The DPO should be consulted at an early stage.

Processing should not begin where a required DPIA has not been completed and appropriate safeguards have not been implemented.

25. Individual Data Protection Rights

Individuals may have rights under data protection law, depending on the circumstances and lawful basis for processing.

These may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to object;
- rights relating to automated decision-making and profiling; and
- the right to data portability in applicable circumstances.

Not every right applies in every circumstance.

Requests should be considered on their individual circumstances and the applicable exemptions.

26. Subject Access Requests

An individual may make a Subject Access Request (SAR) asking for access to their personal information.

A SAR can be made verbally or in writing.

Staff who receive a SAR must forward it promptly to the DPO.

The DPO will coordinate the response.

Remedicare may need to verify the identity of the requester where reasonably necessary.

Remedicare will normally respond without undue delay and within one calendar month of receiving the request, subject to the applicable legal requirements.

Where a request is complex or involves multiple requests, the response period may be extended where permitted by law. The requester will be informed where an extension applies.

Remedicare may refuse or restrict access to information where a lawful exemption applies.

Examples may include information where disclosure would:

- adversely affect the rights of others;
- prejudice a safeguarding or legal investigation;
- reveal confidential information belonging to another person;
- involve legally privileged information; or
- fall within another applicable statutory exemption.

Any refusal or restriction will be considered on its specific circumstances and explained where legally required.

27. Children's Subject Access Requests

Personal data relating to a child belongs to the child rather than automatically belonging to their parent or carer.

A parent or person with parental responsibility may make a request on behalf of a child in appropriate circumstances.

Remedicare will consider:

- the child's age;
- their maturity;
- their understanding;
- their ability to understand the request;
- the nature of the information;
- whether the child has expressed a view;
- parental responsibility;
- the potential impact of disclosure; and
- any safeguarding concerns.

There is no automatic age at which a child is considered capable or incapable of exercising their rights.

Where appropriate, Remedicare may seek the child's views before responding to a parental request.

Where disclosure would not be in the child's best interests or another legal exemption applies, information may be withheld or redacted.

28. Requests from Parents and Carers

Parents and carers may request information about a child, but a request must be considered in accordance with data protection law and the child's rights.

A parent does not automatically have a right to receive:

- another person's personal information;
- confidential information about staff;
- information relating to another child;
- safeguarding information that should not be disclosed;
- information protected by an applicable exemption; or
- all information held about their child without appropriate consideration of the child's own rights.

Requests should be referred to the DPO where there is any uncertainty.

29. Rectification and Other Rights Requests

Individuals may ask Remedicare to correct inaccurate information.

Requests to:

- rectify information;
- erase information;
- restrict processing;
- object to processing;
- withdraw consent; or
- exercise another data protection right

should be referred promptly to the DPO.

The DPO will determine whether the request applies and what action is legally required.

30. Data Protection Complaints

Remedicare will provide a clear way for individuals to raise a data protection complaint.

Data protection complaints should be sent to:

Daniel Nicholson – Data Protection Officer

Daniel.Nicholson@Remedicare.co.uk

Remedicare will:

- acknowledge receipt of a data protection complaint within 30 days;
- make appropriate enquiries without undue delay;
- keep the complainant informed where appropriate;
- provide the outcome without unjustifiable or excessive delay; and
- keep appropriate records of the complaint and outcome.

Where a complaint identifies a weakness in Remedicare's processes, Remedicare will consider whether changes, training or other corrective action are required.

This data protection complaints process is separate from:

- employment grievances;
- general complaints;
- safeguarding concerns;
- whistleblowing;
- disciplinary matters; and
- complaints about the quality of an education placement.

However, matters may overlap and may need to be considered under more than one procedure.

Individuals who remain dissatisfied may complain to the Information Commissioner's Office.

31. Data Protection and Safeguarding

Data protection must not be used as a reason to prevent appropriate safeguarding information sharing.

Where a safeguarding concern exists, staff must follow the Child Protection and Safeguarding Policy.

The DSL and DPO should work together where a safeguarding matter also raises significant data protection considerations.

Safeguarding information should be:

- accurate;
- factual;
- proportionate;
- securely stored;
- accessed only by appropriate individuals; and
- shared only where necessary and lawful.

Staff should avoid recording assumptions, opinions or unnecessary personal information as fact.

Where possible, records should distinguish between:

- facts;
- information reported by another person;
- professional opinion; and
- actions taken.

32. Data Protection and SEND / Health Information

Remedicare may process sensitive information relating to:

- disability;
- SEND;
- EHCPs;
- communication needs;
- medical conditions;
- medication;
- mental health;
- physical health;

- allergies;
- behaviour and regulation;
- social care involvement; and
- safeguarding.

This information must only be accessed by staff who need it for their role.

Staff should not discuss a child's health, SEND or family circumstances in areas where unauthorised individuals may overhear.

Where information is particularly sensitive, additional access restrictions may be applied.

33. Confidentiality

Confidentiality is an important professional responsibility.

However, confidentiality is not absolute.

Information may need to be shared where:

- there is a safeguarding concern;
- there is a risk of harm;
- there is a legal requirement;
- there is a lawful basis for sharing;
- it is necessary to deliver the child's provision;
- it is necessary to protect staff or others; or
- another legitimate and proportionate reason applies.

Staff must not promise a child, young person, parent, colleague or professional that information will never be shared.

34. Data Protection Training

All staff will receive appropriate data protection training as part of induction and ongoing professional development.

Training will cover areas relevant to Remedicare, including:

- UK GDPR and the Data Protection Act 2018;
- confidentiality;
- information sharing;
- safeguarding;
- data breaches;
- secure use of technology;
- email;
- passwords;
- personal devices;
- photographs;
- CCTV;
- record keeping;
- individual rights; and
- data protection responsibilities.

Additional training may be provided where staff have specialist responsibilities.

35. Monitoring and Compliance

Remedicare will monitor compliance through:

- internal checks;
- staff training;
- audits;
- review of data breaches;
- review of data protection complaints;
- DPIAs;
- information governance reviews;
- contract and supplier checks;
- review of access permissions; and
- DPO advice and recommendations.

Where a staff member deliberately or negligently breaches data protection requirements, Remedicare may take appropriate management or disciplinary action.

Any action will be proportionate and consistent with Remedicare's Staff Code of Conduct, Staff Concerns & Conduct Protocol and Disciplinary Procedure.

36. Related Remedicare Policies and Procedures

This policy should be read alongside:

- Child Protection and Safeguarding Policy;
- Staff Code of Conduct;
- Staff Concerns & Conduct Protocol;
- Whistleblowing Policy;
- Disciplinary Procedure;
- Grievance Procedure;
- Health and Safety Policy;
- First Aid and Administration of Medicines Policy;
- Online Safety Policy;
- Complaints Procedure;
- Safer Recruitment Policy;
- Educational Visits / Off-Site Activities Policy;
- Transport arrangements; and
- relevant privacy notices.

Where a safeguarding concern arises, the Child Protection and Safeguarding Policy takes priority in relation to immediate safeguarding action.

37. Accountability and Review

Remedicare will maintain appropriate records to demonstrate compliance with data protection law.

This policy will be reviewed at least annually and sooner where there are:

- changes to legislation;
- significant ICO guidance updates;
- changes to Remedicare's services;
- new technology;
- significant data protection incidents;
- changes to commissioning requirements; or
- changes to the information processed by Remedicare.