Raedwald Trust

connection learning without exception resilience respect

Data Protection Policy

Policy Details	
Person Responsible for this Policy	**Angela Ransby**
Policy Author	**Angela Ransby**
Date to Trust Board	**September 2026**
Date Ratified	
Review Date	**September 2027**
Policy displayed on website	**YES**

CEO Signature	**Angela Ransby**
Trust Board Signature	**Alan Whittaker**

Updates Made	Date

Table of Contents

1. Policy statement

1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an academy trust (Trust"), we will collect, store, and process personal data about our pupils, workforce, parents, and others. This makes us a data controller in relation to that personal data.

1.2. We are committed to the protection of all personal data and special category personal data.

1.3. The law imposes significant fines for failing to lawfully process and safeguard personal data. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

1.4. All data users must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

2. About this policy

2.1. The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'data protection legislation').

2.2. This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3. This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

3. Definition of data protection terms

All defined terms in this policy are

Term	Definition
Biometric data	Is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye, or information about a person's voice or handwriting.
Biometric recognition system	Is a system that operates automatically (electronically) and: • Obtains or records information about a person's physical or behavioural characteristics or features; and Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system.
Data	Is information, which is stored electronically on a computer, or in certain paper-based filing

	systems.
Data subjects	For the purpose of this policy includes all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal data	Means any information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data controllers	Are the people who, or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data users	Are those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy, and any applicable data security procedures, at all times.
Data processors	Include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data protection legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR and the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) (as amended by the Data (Use and Access) Act 2025; and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended, and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.

Data protection impact assessment (DPIA)	A tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The ICO also has guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/.
Information Commissioner's Office (ICQ)	In the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Privacy notices	Where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as data controller and those of the DPO, the purpose, or purposes, and legal basis for which we intend to process that personal data, the types of third parties, if any, with which we will share, or to which we will disclose that personal data, whether the personal data will be transferred outside the UK and if so, the safeguards in place, the period for which their personal data will be stored, by reference to our [data retention policy], the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making, and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
Processing	Is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing

	also includes transferring personal data to third parties.
Special category personal data	Includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, sexual orientation or genetic or biometric data.
Workforce	Includes any individual employed by the Trust such as staff and those who volunteer in any capacity including Trustees/members/ parent helpers.

4. Data users

4.1. The Trust board has overall responsibility for ensuring that the Trust complies with its obligations under data protection legislation. The board of trustees and management are responsible for ensuring all Trust Personnel comply with this Data Protection Policy and are responsible for implementing appropriate practices, processes, controls and training to ensure such compliance.

4.2. The Chief Financial Officer is responsible for day to day implementation of this policy.

4.3. The Head Teacher has day-to-day responsibility in each academy, or the deputy in their absence. The Head Teacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

4.4. All staff are responsible for:

4.4.1. Ensuring that they comply with the Trust's IT and Communications Systems Policy (found in the Staff Handbook) and that:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- Papers containing confidential personal data are not left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Personal data is not in the view of others when being used;
- Computer screens are locked when unattended;
- Personal data is only held on the trust network or a trust issued device (laptop, USB memory stick or other removable media) which is encrypted, password protected, kept in a locked location when not in use;
- Passwords are not shared;
- Passwords comply with the complexity requirements, are changed regularly and different passwords are used for separate systems and devices. A unique password must be used for email accounts;
- Personal data is only shared where necessary and in accordance with trust policy, internally by sending a link to a document on the network, externally using encrypted email;
- Personal data is not disclosed accidentally or otherwise, to any unauthorised third party;
- Personal data is securely disposed of when it is no longer required and in accordance with the document retention schedule.
- Where personal information needs to be taken off site (in paper or electronic form), it is signed out and in from the school office.

4.4.2 Ensuring that they only access data that they have authority to access and only for authorised purposes;

4.4.3 Informing the Chief Financial Officer of any changes to their personal data, such as a change of name, address, or updated relevant medical circumstances;

4.4.4 Contacting the Chief Financial Officer if they:

- receive a Subject Access Request
- have questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- have any concerns that this policy is not being followed
- are engaging in a new activity that involves personal data
- need help with any contracts or sharing personal data with third parties.

4.4.5 Notifying the Chief Financial Officer immediately in the event of discovering a data breach.

5. Data Protection Officer

5.1. As a Trust, we are required to appoint a data protection officer ("DPO"). Our DPO is Tracey Riches, Clear 7 Consultancy.

5.2. The DPO is responsible for informing and advising the Trust about data protection legislation, ensuring compliance with the data protection legislation and with this policy. Any questions about the operation of this policy, or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

5.3. The DPO is also the central point of contact for all data subjects, the Information Commissioner's Office ("ICO") and others in relation to matters of data protection.

6. Our data protection commitments

6.1. We are dedicated to ensuring that personal data is processed in alignment with the legal principles of data protection.

6.2. We implement a strategy focused on "Data Protection by Design and Default".

6.3. We can prove our adherence to data protection legislation.

6.4. Data subjects are well informed about how and why we use their data, and they can exercise their rights regarding their data.

6.5. We share personal data only when it is fair and lawful, ensuring that any data sharing is conducted securely.

6.6. We handle and report all personal data breaches, including minor ones, effectively to mitigate any potential risks and to improve our practices.

7. Data Protection Principles

7.1. Anyone processing personal data must comply with the data protection principles. We will comply with these principles in relation to any processing of personal data by the Trust.

7.2. The principles provide that personal data must be:

7.2.1. Processed fairly, lawfully, and transparently in relation to the data subject. This means that we only use personal data with respect for the individual who it relates to, in line with the legal grounds for processing, and we inform data subjects on how their personal data is processed including, among other ways, in our privacy notices.

7.2.2. Processed for specified, explicit, and legitimate purposes, and in a way which is not incompatible with those purposes. This means that if we collect personal data for one purpose and then need to use it for another reason, we will ensure that new purpose is compatible with the original reason for processing.

7.2.3. Adequate, relevant, and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required.

7.2.4. Accurate and up to date. This means that we will try to ensure that personal data is accurate when we collect it and kept up to date over time.

7.2.5. Not kept for any longer than is necessary for the purpose. This means that we will only keep personal data for as long as is necessary in accordance with our [Data Retention Policy]; and

7.2.6. Processed securely using appropriate technical and organisational measures. Our measures include; technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and

encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

7.3. Personal data must also:

7.3.1. Be processed in line with data subjects' rights.

7.3.2. Not be transferred to people or organisations situated in other countries without adequate protection.

8. Legal grounds for processing

8.1. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. We will normally process personal data under the following legal grounds:

8.1.1. Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.

8.1.2. Where the processing is necessary to comply with a legal obligation that we are subject to.

8.1.3. Where the processing is necessary in order to protect the vital interests of a data subject or another individual.

8.1.4. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest.

8.1.5. Where the processing is necessary for the purposes of a recognised legitimate interest as set out in Annex 1 of the GDPR.

8.1.6. Where we are pursuing legitimate interests, (or the legitimate interests of a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of data subjects; and

8.1.7. Where none of the above apply, then we will seek the consent of the data subject to the processing of their personal data.

8.2. When special category personal data is being processed, then an additional legal ground must apply to that processing. We understand that for certain types of processing of special category personal data, we must have, and comply with, an appropriate policy document. Our special category personal data policy is our appropriate policy document for these purposes.

8.3. We will normally only process special category personal data under following legal grounds:

8.3.1. Where the processing is necessary for employment law purposes, for example, in relation to sickness absence.

8.3.2. Where the processing is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment.

8.3.3. Where the processing is necessary for health or social care purposes, for example, in relation to pupils with medical conditions or disabilities; and

8.3.4. Where none of the above apply, then we will seek the explicit consent of the data subject to the processing of their special category personal data.

8.4. We will inform data subjects of the above matters by way of appropriate privacy notices, which shall be provided to them when we collect the data, or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

8.5. If any data user is in doubt as to the legal ground for processing personal data for any purpose, then they must contact the DPO before doing so.

Vital interests

8.6. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not able to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

8.7. Where none of the other bases for processing set out above apply, then the Trust must seek the consent of the data subject before processing any personal data for any purpose.

8.8. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

8.9. When pupils and/or our workforce join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

8.10. In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

8.11. We will generally seek consent directly from a pupil who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances, and therefore we may be required to seek consent from an individual with parental responsibility.

8.12. If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

8.12.1. Inform the data subject of exactly what we intend to do with their personal data.

8.12.2. Require them to positively confirm that they consent – we cannot ask them to opt out rather than opt in; and

8.12.3. Inform the data subject of how they can withdraw their consent.

8.13. Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent. We will ensure that it will be as easy for the data subject to withdraw their consent as it was to give it.

8.14. Consent may need to be refreshed where we need to process the personal data for a different and incompatible purpose, which was not disclosed when the consent was first considered by the data subject.

8.15. The DPO must always be consulted in relation to any consent form before consent is obtained.

8.16. A record must always be kept of any consent, including how it was obtained and when.

9. Data subjects' rights

9.1. In addition to the right to be informed and the right to withdraw consent, we will process all personal data in line with data subjects' rights, in particular their right to:

9.1.1. Request access to any personal data we hold about them.

9.1.2. Object to the processing of their personal data, including the right to object to direct marketing.

9.1.3. Have inaccurate or incomplete personal data about them rectified.

9.1.4. Restrict processing of their personal data.

9.1.5. Have personal data we hold about them erased.

9.1.6. Have their personal data transferred; and

9.1.7. Object to the making of decisions about them by automated means.

9.2. The rights available to data subjects will depend on the lawful basis for processing, for example, where personal data is processed under the lawful basis of public task, then the data subject cannot withdraw consent for such processing, but they can exercise the right of objection.

9.3. Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under data protection legislation and the guidance given by the ICO in respect of individuals seeking to exercise their rights.

9.4. We will consider data subject requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

9.5. Where we are unable to grant data subjects any requests made as part of their rights, for example, where we are unable to delete data as we are required to retain it in relation to any claim or legal proceedings, we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Trust and to the ICO at the time that we inform them of our decision in relation to their request.

9.6. The DPO must be consulted in relation to any data subject rights request.

<u>The right of access to personal data</u>

9.7. Data subjects may request access to the personal data we hold about them and which we are able to provide based on a reasonable and proportionate search for that personal data. Such requests will be considered in line with the Trust's subject access request procedure.

9.8. To help individuals exercise this right, the Information Commissioners' Office has an online form: Make your subject access request | ICO. We ask that Subject Access Requests (SARs) are made using this form so that we can ensure that we provide the information you would like. However SARs can also be made verbally or by letter or email.

Data protection by design and default

9.9. The Trust will consider and comply with the requirements of data protection legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

9.10. In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a data protection impact assessment ("DPIA"). This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing, or there is a change in our existing ways of working.

9.11. The Trust will complete a DPIA of any such proposed processing, and has a template document, which ensures that all relevant matters are considered. We may also carry out DPIAs where one is not legally required, as a matter of good practice.

9.12. The DPO should always be consulted as to whether a DPIA is required, and if so, how to undertake that assessment. The DPO must always be consulted where personal data is to be transferred to different countries to ensure adequate protection is in place.

10. Automated decision making and profiling

10.1. The Trust does not routinely make decisions about individuals solely by automated means. Examples of automated processing that may be used within an educational setting include:

10.1.1. Admissions systems applying oversubscription criteria.

10.1.2. Recruitment systems filtering or scoring applications.

10.1.3. Behaviour or safeguarding systems identifying patterns or risks.

10.1.4. Assessment platforms that automatically mark or analyse pupil performance.

10.2. Where automated processing produces outcomes that inform or influence decisions, the Trust will seek to ensure that meaningful human involvement such as review, oversight, or the ability to amend outcomes, is applied as part of the decision-making process.

10.3. Where a decision is made solely by automated means and produces legal or similarly significant effects on a data subject, the data subject has the right to:

10.3.1. Be informed that such a decision has been made.

10.3.2. Make representations about the decision.

10.3.3. Request that a human review the decision; and

10.3.4. Contest the outcome of the decision.

10.4. The Trust will ensure that appropriate processes are in place to receive and respond to such requests in a timely manner.

10.5. Where automated decision-making involves the processing of special category personal data, such processing will only take place where:

10.5.1. The individual has given explicit consent; or

10.5.2. The processing is necessary for reasons of substantial public interest and is either: (i) necessary for entering into, or performing, a contract between the individual and a controller; or (ii) required or authorised by law.

10.6. The Trust will keep its approach to automated decision-making under review and will seek further advice where necessary, particularly in relation to new technologies or AI-based systems. Where the Trust's processing activities are also subject to EU GDPR, individuals may hold broader rights in this area, and the Trust's privacy notices will reflect the applicable legal framework accordingly.

11. Data security

11.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

11.3. Security procedures include:

11.3.1. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)

11.3.2. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO guidance on the disposal of IT assets.

11.3.3. Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by, and that they 'lock' or log off from their laptop when it is left unattended.

11.3.4. Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers.

11.4. Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

12. Personal data breaches

12.1. The Trust recognises that a breach of personal data could happen, despite our policies, procedures, and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

12.2. The Trust has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of personal data.

12.3. On finding, or causing a breach, or potential breach, the Chief Financial Officer must notify the Data Protection Officer and complete the Data Breach template on the secure portal within 24 hours of discovery to enable compliance with the requirement to notify the regulator of high risk breaches within 72 hours.

12.4. Guided by the DPO, the CFO will;

12.4.1. Alert the CEO and the Chair of Trustees;

12.4.2. Make all reasonable efforts to contain and minimise the impact of the breach, assisted by the relevant staff members or data processors where necessary;

12.4.3. Document the breach and related decisions;

12.4.4. Capture lessons learned to evaluate how the breach occurred, the success of the response and any improvements to policies and procedures to avoid the situation from happening again.

12.5. The DPO will;

12.5.1. Assess the potential consequences, based on how serious they are and how likely they are to happen;

12.5.2. Decided whether the data subject needs to be notified of the breach;

12.5.3. Decided whether the breach must be reported to the ICO and if so, will notify the ICO within 72 hours of the breach being identified.

13. Disclosure and sharing of personal information

13.1. We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the local authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

13.2. The Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

13.3. Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of personal data.

13.4. In some circumstances we will not share safeguarding information. Please refer to our child protection policy.

14. Data processors

14.1. We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction.

14.2. In order that these services can be provided effectively, we are required to transfer personal data of data subjects to these data processors.

14.3. Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

14.4. Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor to ensure compliance with the data protection legislation, and compliance with the rights of data subjects.

15. Images and videos

15.1. Parents and others attending Trust events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

15.2. The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

15.3. The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

15.4. Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment, and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

16. Video surveillance

The Trust operates a CCTV system. Please refer to the Trust CCTV Procedure.

17. Biometric data

17.1. The Trust may use biometric data (such as facial recognition or fingerprint data) to secure laptops and mobile telephones issued to employees for business use. This data is stored locally on the device and is used solely to authenticate the assigned employee and prevent unauthorised access.

17.2. All such devices are encrypted to safeguard both business and personal data. Biometric data is not transmitted to or stored on central servers, and is automatically deleted from the device when it is reset or returned at the end of employment

18. Complaints

18.1. Data subjects have the right to make a complaint to the Trust if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our DPO.

18.2. When dealing with complaints relating to data protection, we shall:

18.2.1. Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust.

18.2.2. Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate.

18.2.3. Inform the complainant about progress of the complaint; and

18.2.4. Inform the complainant of the outcome of the complaint.

19. Related policies and documents

This Data Protection Policy is linked to:

- The freedom of information publication scheme
- IT and Communications Systems Policy (found in the RT Staff Handbook)
- CCTV Procedure
- Retention Schedule (available on the RT website)

20. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.