# Frequently Asked Questions

This document summarises the frequently asked questions received by the RCSLT in relation to the General Data Protection Regulation (GDPR).

**Please note:** The information provided is for guidance only and does not constitute legal advice. The RCSLT is not in a position to offer individual advice on the application of the GDPR and you should seek advice from your employer, or take legal advice if you are self-employed.

## GDPR guidance for healthcare professionals

**Has there been any guidance published specifically on the implications of GDPR for healthcare professionals?**

To date, there has been limited guidance published from national organisations with expertise in this area about what the GDPR means for healthcare professionals.
The Information Commissioner's Office (ICO) has produced a number of resources to support compliance with GDPR, and will continue to expand guidance on both GDPR and the Date Protection Act 2018 for many months to come. Most ICO guidance is not sector specific (as the laws they regulate are not sector specific), but they do have a webpage aimed at the health sector: https://ico.org.uk/for-organisations/health/. Their main GDPR Guidance can be accessed here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Information Governance Alliance, a department of NHS Digital, have published a number of resources on GDPR developed by England's national GDPR working group: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

While the national GDPR working group is chaired by NHS England, the guidance is being developed to support the NHS, social care and partner organisations, and the guidance will be useful to SLTs working across different organisations across the UK.

The British Medical Association have also developed some open-access resources about GDPR for healthcare professionals:
https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr

**Is the RCSLT responsible for implementing the GDPR for speech and language therapists?**

The responsibility for implementing the GDPR lies with the Data Controllers and Data Processors. Individual speech and language therapists need to identify which of these roles they are operating in and what their duties are. The Information Commissioner's Office and the RCSLT can offer advice and guidance but they cannot implement the GDPR on your behalf. This is because the data principles covered by the GDPR will have a unique application to your data processing activity. The RCSLT is not in a position to offer individual advice on the application of the GDPR and you should seek advice from your employer, or take legal advice if you are self-employed.

For more information on establishing your role and responsibilities in Data Protection legislation, see:

- ICO Summary of GDPR principles: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/
- ICO Advice for small organisations: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/
- ICO Data Controllers Checklist https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/
- ICO Data sharing and subject access checklist https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-sharing-and-subject-access-checklist/
- Article 29 working party – Guideline on Data Protection Officers http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

**Do the RCSLT have templates for consent/ privacy policies that comply with the GDPR regulations?**

The RCSLT are not professional experts in information governance, and we have, therefore, provided guidance to our members in terms of signposting to official information governance authorities, such as the Information Commissioner's Office and the Information Governance Alliance.

Please be aware that in communicating with clients and staff any requests for consent need to be clearly delineated from your privacy notice information.

The following checklists from the ICO cover consent and privacy:

- ICO Privacy information checklist: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

- ICO Data Protection Impact Assessments: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- ICO Data Protection Impact Assessment Template: https://ico.org.uk/media/for-organisations/documents/2258857/dpia-template-v1.docx
- ICO Checklist for Consent as a lawful basis for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

**The RCSLT is directing members to the ICO for information and the ICO is directing members back to their professional body as they are unable to provide advice from a therapist's perspective. Who can provide us with more specific guidance?**

Both RCSLT and the ICO provide guidance about the GDPR but one of the core pillars of the GDPR is accountability. Whilst the RCSLT and ICO are accountable for the implementation of the GDPR to their own data processing activities, you are accountable for yours. As national bodies, neither the ICO nor RCSLT can assume knowledge of your specific local procedures. Application of the GDPR requires it to be applied in a manner that is specific, granular and transparent. You are advised to follow the guidance provided by both organisations and create your own local standards and documentation for data protection.

The RCSLT is continuing to develop more tailored guidance for speech and language therapists, including resources to support members in independent practice.

These resources may be helpful:

- Information Governance Alliance: GDPR guidance on accountability and organisational priorities - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
- Information Governance Alliance: GDPR implementation checklist - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
- ICO key definitions for GDPR: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/
- ICO Summary of GDPR principles: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/
- The Information Commissioners Office has an extensive range of checklists and tools available to support you. Visit www.ico.org.uk

**Who 'owns' personal data?**

The General Data Protection Regulation is concerned with the handling of personal data. It doesn't specifically discuss 'ownership' of data, however it aims to give control of personal data back to the individual by clearly defining individual's rights in respect to the personal data organisations hold on them. These include:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

The Data Controller must also demonstrate compliance with the data protection principles discussed in Article 5 of the GDPR. These principles also strengthen the individuals control over the use of their personal data.

More information on the role and rights of data subjects and controllers can be found in the RCSLT's General Data Protection Regulation supplementary guidance.

**What are the implications of the GDPR for SLTs conducting research?**

The NHS Health Research Authority has developed guidance about the impacts of the GDPR on handling research data: https://www.hra.nhs.uk/hra-guidance-general-data-protection-regulation/. They have also developed templated to support organisations with informing research participants about how their personal data is being used: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/

## Record management

**As a data controller, do I need to register with the ICO?**

Registration is no longer required; this has been replaced by a new compulsory fee to the ICO. Existing registrations will run their current term and then the data controller will swap on to the new fee system.

**Does the GDPR affect how long documentation should be kept?**

Neither GDPR nor Data Protection Act 2018 set any specific retention periods, but simply require that data is not kept in identifiable form for longer than is 'necessary'; article 5 of the GDPR requires that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals".

In deciding how long is 'necessary', you can ask yourself the following three questions:

- Is there a law specifying how long I keep this data?
- If not, is there an industry standard I should follow?
- If not, how long do I need this data for my legitimate business purposes?

The GDPR must be considered within the wider context of UK law; information governance is covered by a multitude of legislation and standards. The RCSLT webpages provide further information on the relevant UK and national legislation and record keeping guidance.
You should also refer to any local record management policies and procedures.

**There is a right of erasure under GDPR, however is it correct that patients don't have that right when it comes to healthcare case notes? If someone turns around and asks to destroy all of the notes on their child, under GDPR laws, then what would happen?**

GDPR provides that the right to erasure does not apply to health and care data in the following circumstances:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

The right to erasure actually has quite a narrow application, so even if you receive a request relating to information that does not fall within the health and care categories listed above, it's a good idea to check the ICO web guidance before deciding whether or not you should comply: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

**What should happen to clinical data when a contract ends?**

- Where the therapist is employed by the organisation, it would be difficult for the therapist to justify keeping a copy of all the notes since the organisation (as Data Controller) would be ultimately liable. However it may be appropriate in specific instances if the therapist can demonstrate a good enough reason for continued access e.g. an ongoing case. Before a therapist leaves the employment of a school there needs to be a professional discussion on the long-term storage requirements of the notes to satisfy professional obligations, and this should be documented.
- Where a contract between an organisation and an independent therapist/practice comes to an end then the notes can be handed over at the point of transfer, but it would be acceptable for the therapist/practice to keep a copy (justified for the purposes of future liability). Since there are two Data Controllers it would however be necessary for one of them to assume overall responsibility for the notes (the master copy) in case the Data Subject requests any amendments or additions to be made in the future.

**Once an SLT has deceased, what happens with the case notes?**

If there is clinical need for the notes to be retained after the SLT has passed away then data controller status would fall to the organisation taking on the clinical oversight. Where notes are no longer needed for a clinical purpose they must be securely destroyed.

**What is best practice for the handover of notes if this wasn't documented previously?**

First, identify who is the Data Controller. If it is the therapist then responsibility for the retention of notes rests with them. If the Data controller responsibilities are shared then a documented agreement should be drawn up e.g. that the school will keep the notes but will honour any future request for access from the therapist.

**In a situation where the SLT is not the data controller, can they retain a copy of the notes at the end of the contract/employment?**

It would be down to the data controller to decide whether this is appropriate. You would need to be very clear about the purpose of duplicating notes and whether there would be any negative impact on the individual's care (e.g. reasons for the SLT keeping a copy might include liability). There is a significant IG risk associated with duplicated notes and ideally all options to avoid it should be explored. If unavoidable, a risk assessment should be completed, including details of how additions to the original will be managed, secure storage and disposal.

In the case of joint data controllership where the school retains the notes, the original agreement between the SLT and the school might include a clause that says that the school will allow the SLT to access the notes if required once the contract has terminated for specific purposes e.g. liability purposes.

**Can you advise me on the right to having data destroyed for supervisees. Is there any reason to keep meeting notes once no longer providing supervision? How long should personal data be kept after supervision ends and does the supervisee have the right to have data destroyed immediately on request?**

GDPR does not set any specific retention periods, but simply requires that data is not kept in

identifiable form for longer than is 'necessary'. In deciding how long is 'necessary', ask yourself the following three questions:

- Is there a law specifying how long I keep this data?
- If not, is there an industry standard I should follow?
- If not, how long do I need this data for my legitimate business purposes?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

## Lawful processing

**The GDPR requires me to identify the lawful basis for processing personal data. What does this mean?**

This is similar to the 'conditions for processing' under the Data Protection Act 1998. When thinking about each processing activity, you should consider the purpose and the most appropriate lawful basis for that given activity. Personal data relating to health is 'special category data' under the GDPR. For this type of data, you are required to identify the lawful basis for processing under Article 6 and a separate condition for processing special category data under Article 9. The ICO provides guidance on special category data: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. You will also need to a condition for processing under Article 9 for other types of special category data that you handle.

There is no single basis for processing that is 'better' than others; the most appropriate lawful basis will depend on the specific purposes and the context of the processing. The ICO provides guidance on this: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Things to consider:

- This applies to any personal data you process, not just that of your patients. Other types of data, e.g. staffing data, should be considered.
- You should state the lawful basis for processing data in your privacy notice.
- If you use consent as the lawful basis for processing, ensure that your processes for recording and managing consent meet the GDPR standards. The GDPR has tighter requirements for consent to process and store data. For example, you must be able to demonstrate that you have consent and the individual must be able to withdraw consent easily.

- RCSLT GDPR guidance: https://www.rcslt.org/members/delivering-quality-services/information-governance/information-governance-guidance#section-21
- ICO Lawful basis for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

**Precisely which lawful basis should SLTs operate under?**

There are six lawful bases for processing data. These are consent, lawful obligation, contract, vital interests, public task and legitimate interests. The data controller must choose which basis is the 'best fit' for each type of data before processing commences. The lawful basis for processing may vary depending on what data you are processing and for what purpose. You must clearly document and inform data subjects of your lawful basis and intended purposes for processing the personal data. You should be aware that the lawful basis chosen will influence the individual's data protection rights. Appropriate procedures must be in place to meet these rights as required.

For more information on establishing which lawful basis pertains to your activity refer to:

- ICO Lawful basis for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
- ICO Lawful basis interactive guidance tool: https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/
- ICO Legitimate interests: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/
- ICO Checklist for Legitimate interests as a lawful basis for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

**Is 'legitimate interests' the most appropriate lawful basis?**

Data controllers are responsible for identifying the most suitable category for each data type. The GDPR stresses, there is no one fit for all. 'Legitimate interests' is an available lawful basis, but in the context of processing healthcare data, it should be noted that it is not then appropriate to use (2)(h) – "processing is necessary for…the provision of health or social care or treatment…" under article 9. This is available to speech and language therapists. A lawful basis under article 6 that can be used with this, where appropriate, is 'public task'(1)(e): "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". It is important to note that this is only appropriate where the speech and language therapist is contracted by a public body. In situations where the contract is between the SLT and the client (or parent/carer, where appropriate), another lawful basis should be considered. It may be appropriate to use 'contract' (1)(b): "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". It is emphasised that the most appropriate lawful basis will depend on the context of the processing.

**I am an independent SLT operating as a sole trader, providing predominantly one-to-one private speech and language therapy under contract with the client directly (or the parent/carer). I have identified that an available condition for processing special category data under article 9 of the GDPR is 9(2)(h) "processing is necessary for … the provision of health or social care or treatment" and that an available lawful basis under article 6 is 6(1)(b) "contract". Individuals have a right to erasure under 6(1)(b) but 9(2)(h) is exempt from the right to erasure. Does the right to erasure apply?**

GDPR provides that the right to erasure does not apply to health and care data in the following circumstances:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to

a legal obligation of professional secrecy (e.g. a health professional).

The ICO has developed guidance on right to erasure: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

**What wording should I use for privacy policies – is it legal or legitimate reasons to storing data?**

The GDPR outlines six lawful bases for processing. Two of these contain the terms you are questioning:

- **Legal obligation** – processing the data is necessary to comply with common or statuary law. You must identify and document the specific legal provision.
- **Legitimate interests** – necessary and acceptable interests of the data subject/ or third parties. You must identify and document the legitimate interest, show that processing is necessary to achieve it and balance it against the individual's rights and freedoms.

To find out more about Article 6 of the GDPR see **Lawful basis for processing**: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

## Security

**Do emails containing personal data need to be encrypted for GDPR, or is password protection enough?**

The GDPR does not define the security measures you should have in place, but it requests the level of security is appropriate to the risks associated with the data you are processing. Personal data contained in an email can be at risk if, for example, the email is accessed or intercepted by an unintended recipient. This would be a personal data breach. There is a requirement under the GDPR that data breaches are recorded and, in some cases, reported to the ICO, as well as a responsibility to report the breach to the individual. Informing the individual of a breach of personal data is already required under the Duty of Candour.

The RCSLT recommends that emails containing personal confidential information should only be sent to and from secure accounts (as defined by Information Standard Board (ISB)

Standard 1596)).

These include:

- .cjsm.net (criminal and justice)
- .gcsx.gov.uk (local government/social services)
- .hscic.gov.uk (Health and Social Care Information Centre)
- .nhs.net (NHS mail)
- .scn.gov.uk (criminal and justice)

- NB: nhs.uk accounts are not secure.

Emails sent, from or to a secure account, from an insecure account need to be encrypted. The recipient will also need appropriate encryption software to read it. Parent mail and My School Portal are examples of secure platforms that can be used to communicate with parents.

Emails to service users' personal accounts are not secure. Service users without adequately secure accounts should be offered:

- access via a safe space site
- access via a special domain account address
- access via an encryption/decryption mechanism.

**Diaries are used to record entries in terms of visits the SLTs are going to make. Are there any recommendations regarding what SLTs should do in terms of inputting client information (e.g. addresses, full names, date of birth) into diaries in light of GDPR?**

The GDPR does not specifically mention the storage of names/ addresses for this purpose. Diaries are at risk of loss, theft, misplacement and could easily be overseen by a third party. If you are keeping personal data in diaries you need to justify it in acceptable terms, which could be difficult to do under data protection principles. As part of your data review you could explore more secure methods of storing patient details, such as encrypted laptops or other mobile electronic devices. If you work for a larger organisation contact your Data Protection Officer for their advice.

If you have no option but to use hard copy diaries and notes, ensure these are securely stored at all times, especially during transit, and consider devising a code that reduces the risk of the patients' personal information being identified (e.g. only use initials).

Ensure all passwords are robust, never shared and frequently updated.

For more information on data protection principles see:
ICO Summary of GDPR principles: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

## Documentation

**What is a data sharing agreement and when is it used?**

Data sharing agreements are common between health and social care providers. They enable safe and efficient transfer of information between participating organisations.

Data sharing agreements may involve several organisations and are subject to the same data protection laws and requirements. They may also be in place within different branches of a single organisation.

Details on the different types of data sharing can be found in the Data Sharing Code of Practice: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The ICO is currently updating the Data Sharing Code of Practice in light of the new Data Protection Act (2018).