General Data Protection Regulation (GDPR) supplementary guidance

The General Data Protection Regulation (GDPR) is concerned with how we process data. It is mandatory and speech and language therapists are required, by law, to act upon it.

Many of the core principles of the Data Protection Act 1998 remain the same under the GDPR. If you meet the requirements of the current law, you will be well placed to meet the standards of the GDPR; current best practices for data protection should not be too difficult to adapt to the new requirements. One of the pillars of the GDPR is accountability: you are responsible for complying with the GDPR and you must demonstrate that compliance.

This document represents an overview of the GDPR and highlights the key points speech and language therapists should consider. It is emphasised that this information is for your general guidance only and is not intended to be an exhaustive list of things to consider. The information provided does not constitute legal advice. Each speech and language therapist is responsible for understanding how they manage, process and review data in their specific field and be able to demonstrate compliance.

As well as GDPR, the Data Protection Act 2018 took effect from 25 May 2018. This legislation is designed to sit alongside the GDPR. This legislation addresses areas outside of the scope of GDPR and areas that are left to the discretion of the UK. This document will be updated and reviewed to include further guidance from expert sources as it becomes available.

The RCSLT are not professional experts in information governance, therefore, we have provided links throughout this text to official expert sources such as the Information Commissioner's Office (ICO). It is the responsibility of individual speech and language therapists to refer to these primary sources when considering their unique data processing requirements. Members working in larger organisations should contact their Information Governance Department or Data Protection Officer for advice and policies. Members working in small organisations and those working as sole traders should be reassured that there are a number of resources available to help with understanding and complying with the GDPR.

This document is divided into two sections:

Section one provides an overview of the GDPR and advice on actions you should consider to ensure compliance with the new regulations and related resources.
It covers:

Section two looks in more detail at specific aspects of the GDPR which you will need to consider when amending or developing your data protection policies and procedures. Links to resources are provided to help you integrate these into your current data protection practices.
It covers:

What is the GDPR?

The General Data Protection Regulation (GDPR) is concerned with the handling of personal data. It aims to

- give control of personal data back to the individual
- ensure transparency and accuracy

It applies across the European Union (EU) and to those based outside the EU if their services are available in the EU. The GDPR came into force on the 25 May 2018.

The Data Protection Act 2018 sits alongside the GDPR.

Activities to consider undertaking in your organisation:

Raise awareness amongst your colleagues.
The GDPR applies to everyone handling data. They should be aware of the changes and implications. The HCPC standards of conduct, performance and ethics require registrants to understand and practice safe and effective practice in relation to confidentiality and record keeping. Consider how you can effectively disseminate this information. Review mandatory training and induction processes.

Resources

- 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-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

What constitutes personal data?

Personal data is information related to an individual that enables them to be directly or indirectly identified. Legally this person is known as the 'data subject'. Personal data can relate to anything from a name to a photo, email address, phone number, medical information, credit card number, location data or computer IP address.

The GDPR applies to automated personal data, manual filing systems and information waiting to be added into such systems.

Completing an information audit or data mapping exercise can help you find out what personal data your organisation holds, where it is, who it is shared with, how long it is kept and how it is acquired and erased.

Activities to consider undertaking in your organisation

Complete/ review an information audit.
Audit the type of data you hold, the types of processing activities you carry out, the lawful basis for doing so and the retention periods. This includes both patient data and other forms of personal data held by the organisation (e.g. employee data).

Resources

- ICO lawful basis: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
- ICO documentation templates for data controllers and data processors
- ICO Data Protection Impacts Assessment (DPIA): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Who does the GDPR apply to?

The GDPR is relevant to everyone.
There are three key players referred to in the GDPR.

The Data Subject
The individual the data is about.

The Data Processor
Responsible for processing personal data on behalf of the Data Controller. Legally responsible for maintaining records of personal data and processing activities.

The Data Controller
Determines the purpose and means of processing data. Responsible for ensuring the Data Processor complies with the GDPR.

Larger organisations will also have a Data Protection Officer (DPO). Their role is to inform and advise you on data protection regulations, provide advice about Data Protection Impact Assessments, monitor compliance and act as a contact point for data subjects and the supervisory authority. Smaller organisations may wish to appoint an external DPO.

All speech and language therapists need to be aware of their responsibilities as regulated healthcare professionals.

Where speech and language therapists are employed by an organisation, the organisation as a whole will be the data controller. In this situation, it will be the board of the organisation that is accountable in terms of legal enforcement, but each member of the organisation should be aware of their individual responsibilities.

Speech and language therapists who are sole traders or the owners of an independent practice are data controllers in their own right and will be responsible for setting the data protection policies and procedures in their practice. In addition, they should pay an annual fee to the Information Commissioner's Office (ICO) – the new laws have abolished the requirement to register, but continue to require payment of a fee. If you are already registered with the ICO under the previous legislation, you will join the new fee system when your current registration expires. For more information, including on exemptions to the fee, see: https://ico.org.uk/for-organisations/data-protection-fee/

It is important that the data controller role is clear in situations where independent speech and language therapists are contracted by public bodies. Contracts guidance is available from the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

If a data controller uses a data processor, the data processor should only process the data for specific purposes as set out in a contract. An example of where a data processor would be used includes where an independent practice uses a payroll company. In this scenario, the independent practice is the data controller and provides the relevant data about employees, which is stored and used by the payroll company, who is the data processor. A contract between the controller and the processor would be required, which sets out the specifics, including what happens to the personal data at the end of the contract.

Activities to consider undertaking in your organisation

- **Identify who holds which role in your organisation(s), what their responsibilities are and how they are met.**
- **Consider whether you need to update your registration with the ICO.**
- **Consider whether you need to appoint a Data Protection Officer.**
- **Training for key stakeholders.**

Resources

- 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 – Data Protection Officer http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
- ICO GDPR documentation data controller template
- ICO GDPR documentation data processor template

Complying with the GDPR

The requirements of compliance with the GDPR will vary with the type of data being collected, about whom and for whom.

Speech and language therapists should be aware of the following **Data protection principles** under the GDPR (Article 5):

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- 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 shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that the controller will be responsible for and able to demonstrate compliance with these principles.

Speech and language therapy data controllers should identify what information they hold:

- Where is it from?
- What do you do with it?
- Who do you share it with?

Activities to consider undertaking in your organisation:

- **Establish a plan and implementation programme for the GDPR**
  Depending on the size of your organisation, appoint an appropriately skilled person, ensure adequate resources (e.g. time), complete a gap analysis and record a risk register. The Information Governance Alliance (IGA) GDPR implementation checklist is a good resource for larger organisations. The ICO provide specific advice for small businesses (see links in resources).

- **Revise your policies and procedures to ensure that these comply with GDPR**
  Check that all procedures cover the data protection principles and the new rights individuals have under GDPR (e.g. the right to be informed; the right of access). Policies and procedures to review include (but not exclusive to):
  - Data protection impact assessments
  - Consent policies (if using 'consent' as the lawful basis for processing data)
  - Subject access request procedures – be aware of new requirements in terms of timescales and that most requests must be handled free of charge.
  - Procedures in the event of a data breach

- **Review and produce data protection impact assessment**
  Data Protection Impact Assessments (DPIAs) are similar to privacy impact assessments. It has always been good practice to carry out a privacy impact assessment but the GDPR makes DPIAs mandatory in certain circumstances. This includes where there is a high risk to individuals, including the processing of special category data. DPIAs should be conducted and reviewed on a regular basis. If you are familiar with conducting privacy impact assessments it should easy to follow the DPIA process.

- **Review privacy notices**
  The GDPR requires additional information about how personal information is used to be included in privacy notices. When collecting children's data your privacy notice must be written in language that children will understand.

- **Review any data sharing arrangements you have with other organisations.**

Resources

- 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 Data Protection Self-Assessment Tool: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
- ICO Summary of GDPR principles: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/
- ICO Advice for small businesses: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/
- ICO Individual Rights: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
- ICO Right of Access: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
- ICO Right to be informed: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
- Article 29 working party – data breach: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- ICO Consent Guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/
- Article 29 working party – consent: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239
- Article 29 working party – data protection impact assessments: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- ICO How do we carry out a DPIA? https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/

GDPR in the context of wider UK law

It is important to see the provisions of the GDPR within the context of wider UK law. These will impact on your specific application of the GDPR.

Relevant UK and national legislation to be aware of in relation to information governance is summarised on the RCSLT webpages.

For example, you should be aware that:

- A duty of care is placed on health and social care providers to share information under the Health and Social Care Act (2012) section 251B and the common law duty of confidence.
- The Duty of Candour requires individuals are informed of incidents.
- The Information Governance Alliance (2016) Records Management Code of Practice for Health and Social Care provides guidance on record retention standards.
- Patient data, in health, is held under a duty of confidence, allowing for implied consent to be justified for direct care. This wouldn't meet the clear affirmative act of GDPR consent and therefore consent is often not the most appropriate lawful basis for direct care.

Individual Rights

The GDPR provides the following rights to individuals (adults and children) in respect to the personal data that organisations hold about them:

The right to be informed (Article 12-14) – this is a key transparency requirement of the GDPR. You must provide individuals with information on your purpose for processing data, retention periods and who the data will be shared with. The information must be provided in an appropriate accessible format. This information is known as a privacy notice. Details on how to draft one have been provided by the ICO (see link in resources)

The right to access (Article 12 and 15) – individuals have the right to access and have a copy of their personal data. This right is very strong and limited exemptions apply (for example if there are significant safeguarding concerns).

The right to rectification (Article 5, 12, 16 and 19) – individuals can request for incorrect or incomplete information to be amended.

The right to erasure (Article 6, 9, 12, and 17) –also known as 'the right to be forgotten'. The right to erasure is not absolute and only applies in certain circumstances. Health and social service data is identified in the GDPR as a special category in which the right to erasure does not apply so long as the data is necessary for the health and care purpose.

The right to restrict processing (Article 18) – in certain circumstances individuals have the right to request the restriction or suppression of their personal data enabling them to limit how an organisation uses their data.

The right to data portability (Article 13 and 20) – in certain circumstances this enables individuals to request and reuse their electronic data for their own purposes across different services.

The right to object (Article 12 and 21) – Individuals have an absolute right to object to the processing of their personal data for direct marketing purposes and you must comply. Individuals can also object based on their specific circumstances if the processing is for: a task carried out in the public interest; the exercise of official authority vested in you; or your legitimate interests (or those of a third party). In these circumstances the right to object is not absolute and you will need to assess on a case by case basis whether your lawful basis outweighs the individual's objection.

Some of these rights only apply in relation to certain lawful bases for processing. Further information on lawful bases is available in the next section of this guidance.

The Data Protection Act 2018 provides some restrictions on individual's rights, for example in relation to research work. See the Information Commissioner's Office (ICO) website for the most up to date guidance on how to apply the Individual's Rights.

Any requests for information must be completed within one month of the request. The request may be verbal or written. No fee can be imposed. You may decline the request or charge a reasonable fee if the request is repeated or manifestly unfounded. Where a request is particularly complex, you may extend the response time. Please refer to the ICO website for guidance if considering refusing a request, charging or extending the timescale

Any parties the data has been shared with must be individually informed of changes.

Activities to consider undertaking in your organisation:

- **Update your communication materials and internal processes to support individual rights.**
- **Consider establishing a procedure for responding to enquiries about rights.**
- **Revise your subject access procedures.**

Resources

- 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/
- NHS England (2016) Accessible Information Standard: https://www.england.nhs.uk/ourwork/accessibleinfo/
- 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 Preparing for rectification requests checklist: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/
- ICO Preparing and complying with requests for erasure checklist: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/
- ICO Preparing and complying with requests for restrictions: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/
- ICO Preparing and complying with data portability checklist: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

Processing personal data

Lawful basis for processing

The first principle of the GDPR requires that you process information lawfully. The GDPR requires the lawful basis for processing personal data to be identified and documented. The lawful basis for processing is similar to the 'conditions for processing' under the Data Protection Act 1998.

As data and data processing take various formats, there are multiple different lawful bases for processing data.

Data relating to health (and any other sensitive data processed by the organisation) is known as 'special category data' under GDPR and will require two lawful bases to be identified – one under Article 6 and one under Article 9 of the GDPR.

These are the six lawful bases identified in the GDPR under Article 6:

Consent (Art 6(1)(a)) – must be explicit, specific and granular, with any third party data controllers identified. A positive opt in is required and the process by which consent may be withdrawn must be clear. Who, why, what and when must be documented.

Contract (Art 6(1)(b))– processing data is a necessary part a contract with the data subject

Legal obligation (Art 6(1)(c)) – processing the data is necessary to comply with common or statuary law. You must identify and document the specific legal provision.

Vital interests (Art 6(1)(d)) – to protect life. You cannot rely on this if the individual is able to give consent.

Public task (Art 6 (1)(e))– necessary for task/ function with a clear basis in law and in the public interest or excise of an official authority. Relying on this lawful basis requires that it is necessary for the controller to process data for those purposes and that the controller can identify a clear legal basis to do so under UK law.

Legitimate interests (Art 6 (1)(f)) – 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.

Your lawful basis for processing may vary depending on what data you are processing and for what purpose. You may choose more than one lawful basis, or just one, but you must not use a one-size-fits all approach. If your data is to be used for more than one purpose, clear information must be given on each intention.

Examples

- Where the SLT is contracted by a public body with a function to deliver a statutory function (e.g. NHS or local authority), an available basis under article 6 is (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"

- If the contract is between the client/parent/carer and the SLT, or between the SLT and their employees, an available basis under article 6 is (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"

- 'Legitimate interests' (1)(f) could be used by SLTs when processing personal data in advisory function or providing something that is not obligatory (including internal functions such as providing an intranet for staff)

- 'Consent'(1)(a) could be an appropriate lawful basis for marketing purposes.

National bodies, such as the ICO, provide advice on what constitutes lawful processing, but it is the responsibility of the data controller to establish which lawful basis applies to them.

Speech and language therapy data controllers should review existing processes and check which of the GDPR lawful bases for processing apply to them.

To choose the right bases you should consider:

- What is your purpose?
- What are you trying to achieve?
- Do you have a choice over whether to process the data?
- Are you a public authority?
- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the process at any time on request?

You must clearly document and inform data subjects of your lawful basis and intended purposes for processing the personal data (GDPR Article 5 (2), 13, 14 and 24). There is no

standardised form for doing this. You could consider referring to the ICO information on privacy notices and create your own documentation.

The lawful basis that applies to the data should be identified *before* processing begins. It is important to get your choice of lawful basis right from the start. Once a decision is made it would be very difficult to switch bases and maintain the legal requirements of accountability and transparency to the individual. This would risk a breach of Data Protection law.

You should be aware that the lawful basis chosen will influence the **Individual Rights**. Appropriate procedures must be in place to meet these rights as required.

Checklists for lawful basis can be found on the ICO website.

Special category data

Article 9 of the GDPR covers processing special category data.

Special category data is data the GDPR has identified as more sensitive and in need of more protection. It includes healthcare data.

In these cases, a lawful basis (under Article 6) and a special category (under Article 9) must be identified.

GDPR conditions for processing special category data that are most relevant to speech and language therapists are:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
- Processing is necessary to carry out specific rights related to employment, social security and social protection.
- Processing is necessary to protect vital interests when the individual is physically or mentally unable to give consent
- Processing is necessary for legal claims
- Processing is necessary for substantial public interest
- Processing is necessary for preventative or occupational medicine, assessment of working capacity, provision of health or social care treatment, management of health and social care systems
- Processing is necessary for archiving in the public interest, historical research or statistics purposes

Under the Data Protection Act 2018, SLTs fall under the definition of "health professionals" under 195(1)(g):

> "a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England"

An available basis for the processing of health data under article 9(2) is therefore:

> "(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3."

Activities to consider undertaking in your organisation:

- **Update your information asset register to include information on which legal basis (and special category) you have chosen to process data under and why.**
- **Update your communication materials and privacy statements ensuring transparency.**
- **Ensure all staff understand and can explain the reasons for processing data with data subjects.**

Resources:

- ICO Lawful basis for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
- ICO Special Categories (includes the Data Protection Bill proposals): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
- 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 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/
- 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/
- ICO Legitimate interests (includes completing a Legitimate Interests Assessment) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/
- IGA The GDPR guidance on lawful processing: 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

Documentation

The documentation of processing activities is a new requirement under the GDPR. You must keep written records of how you process, retain, share and dispose of data. The record must include the reasons behind these decisions. The ICO can request to look at the documents of data processors and controllers.

Information audits or data mapping exercises can be used to feed into documentation of your data processing activities.

Records must be kept up to date and reflect current activities. Electronic records are usually the most effective way to do this.

Organisations with fewer than 250 employees need only document processing activities that are not occasional, that fall into the 'special categories' or which have high risk to the rights and freedoms of individuals. Larger organisations must document all processing activities.

Under Article 30 of the GDPR you must document the following information:

- Name and contact details of your organisation
- Purpose of your processing
- Description of categories of individuals and categories of personal data
- Details of transfer of data to third parties, including your safeguard mechanism
- Retention schedules
- Organisational and technical security measures

Documentation should also include:

- Records of consent
- Controller-processor contracts
- Location of personal data
- Data Protection Impact Assessment reports
- Records of personal data breaches
- Information required for processing special category data

A Privacy Notice should include:

- Lawful basis for processing
- Legitimate interests for processing
- Individual's rights
- The existence of automated decision making including profiling
- The source of the personal data
  See ICO website for a full list of the mandatory content of privacy notices.

Activities to consider undertaking in your organisation:

- **Revise or establish information asset registers. Include information on Article 6 (lawful process) Article 9 (special categories).**
- **Regularly review and update documentation on data and processes.**
- **Document how information is obtained, stored and transferred**
- **Update communication/ fair processing/ privacy notices ensuring they comply with the GDPR requirements for transparency (Article 13 and 14)**

Resources

- ICO Data Protection Impact Assessments: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
- ICO Data Sharing Code of Practice: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf NB: this document is based on the Data Protection Act 1998, it is due to be updated by the ICO in line with the GDPR
- Information Governance Alliance (2016) Record Management Code of Practice for Health and Social Care: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Security

The GDPR does not define the security measures you should have in place. It requests the level of security is appropriate to the risks associated with the data you are processing. This is because there is no one-size-fits-all measure for information security. You should review the personal data you hold and the way you use it, in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data is compromised.

Article 5 (1)(f) of the GDPR states:

"Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

You must ensure data can only be accessed, altered, disclosed or deleted by those with authorisation to do so. The data must be accurate and complete in relation to the reasons why you are processing it. The data is accessible and usable and if lost there must be a means by which to recover it.

You need to consider:

- Co-ordination of data between people within your organisation
- Access to premises/ systems by anyone outside your organisation
- How you will protect and recover personal data you hold
- Physical security measures: locks/ lighting/ alarms/ doors/ CCTV
- How visitors are supervised
- How paper and electronic confidential waste is disposed of
- How you keep IT and mobile equipment secure

You must keep documentation of security measures in relation to data you process.

Activities to consider undertaking in your organisation:

- **Ensure everyone understands where/ how information is sent/ transferred/ received and how it is protected.**
- **Update organisational policies.**
- **Consider whether a Data Processing Impact Assessment (DPIA) is required.**
- **Seek advice from your Data Protection Officer, if available.**

Resources

- ICO A practical guide to IT security: https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf
- ICO Security checklists: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

Personal data breaches

A personal data breach of security must be reported to your relevant supervisor within 24 hours of its occurrence.

A breach would include:

- Access by an unauthorised third party
- Sending personal data to the wrong recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data
- Deliberate or accidental actions which compromise security

A breach that is likely to pose a risk to people must be reported to the ICO by telephone or via the website within 72 hours of becoming aware of the breach (see https://ico.org.uk/for-organisations/report-a-breach/). However, if you are part of NHS England then report breaches within 24 hours using the NHS England IG Incident Reporting Tool which will automatically notify ICO.

If the breach is likely to put the rights and freedoms of individual at high risk you must inform those directly concerned without due delay.

The Duty of Candour already requires that individuals are informed of breaches of their NHS data.

Failure to report data breaches as required to ICO could result in a significant fine.

Activities to consider undertaking in your organisation:

- **Complete a gap analysis and record major gaps in a risk register.**
- **Develop a compliance plan based on gap analysis and review resource requirements.**
- **Set time scales for reviewing your processes and who will carry these out.**
- **Review incident reporting procedures and ensure all staff are aware of them.**

Resources

- ICO Report a breach: https://ico.org.uk/for-organisations/report-a-breach/
- ICO Guide to the General Data Protection Regulation: Personal Data Breaches: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- NHS Digital Information Governance Toolkit: https://www.igt.hscic.gov.uk

Appendix 1: Action checklist

Prepare

Action	Related Information	✓
Ensure you understand the key principles of the GDPR and the handling of personal data	Pages 3 – 17	
Identify roles and responsibilities in terms of data controller/ processor.	Pages 5 – 6	
Identify local and/ or national resources that can offer support.	Pages 3 – 22	
Identify and allocate appropriate resources to apply the new data protection regulations.		
Raise awareness amongst colleagues about the changes.	Pages 3 – 10	

Review

Action	Related Information	✓
Complete an audit of current data held in an information assets register	Pages 4, 7, 8, 18, 19, 25	
Consider completing a Data Protection Impact Assessment	Pages 8 – 9	
Record major gaps in a risk register	Pages 8, 22	
Review/ update processes for data breaches	Page 21 – 22	
Review/ update processes for data sharing/ security	Page 20	

Revise your processes to ensure they comply with the GDPR

Action	Related Information	✓
Identify lawful basis for processing and special categories as applicable	Pages 13 – 17	
Consider compliance with individual rights and how these are implemented	Page 11	
Consider how data is shared safely and securely between organisations	Pages 7, 18 – 22	
Consider how you respond to subject access and other individual rights requests	Page 8	
Ensure compliance is demonstrated (e.g. as part of your information assets register)	Pages 18, 25	
Consider how you will respond to a possible data breach situation	Pages 21 – 22	

Ensure accountability and transparency

Action	Related Information	✓
Clearly document your processing activities	Pages 18 – 19	
Update/ create a privacy notice	Pages 8, 11, 15, 18, 19	
Ensure accessible information is available to service users	Page 26	
Create a statement of organisational accountability and compliance with the data protection principles	Pages 5 – 8	
Consider using the ICO documentation checklists for data controllers/ processors	page 6	

Raise Awareness

Action	Related Information	✓
Communicate significant changes to staff	Page 3	
Communicate changes to service users	Page 26	
Revise training materials	Page 3	

Appendix 2: Information asset registers

The content of your information asset register will vary dependent on your data processing needs. Relevant headings to consider include:

Name and contact details of data controllers/ processors.	
Data type	
Source of data	
Individuals it applies to	
Purpose of processing	
Lawful process	
Special category	
Individual rights available	
Record of consent (if applicable)	
Location of data	
Retention schedule	
Names of third parties	
Safeguards/ security measures in place	
Review date	

Appendix 3: Accessible Information

Speech and language therapists should ensure information provided about their data collection and processes is accessible to everyone.

Creating accessible information for people with specific language difficulties can be challenging.

Follow accessible information guidelines such as

NHS England (2016) Accessible Information Standard
Stroke Associations (2012) Accessible Information Guidelines

You should consider using:

- a non-serif font, such as Arial
- size 14 minimum
- short sentences structures
- plain language
- picture support of key concepts

More information about accessible information is available on the RCSLT website.

Some images relating to IG can be found here.

A general leaflet on information rights for individuals can be found here.

These images are available under creative commons licence and can be used without attribution in the creation of your own information leaflets. Copyright remains with Aphasia Friendly Resources.

Furthermore, if in Wales, consider any Welsh Language obligations that may apply to your organisation.

ICO 'Your Data Matters' campaign materials can be downloaded and used free of charge: https://ico.org.uk/for-organisations/resources-and-support/your-data-matters-campaign/

Appendix 4: Frequently asked questions

RCSLT have compiled a list of frequently asked questions and their responses related to data protection.