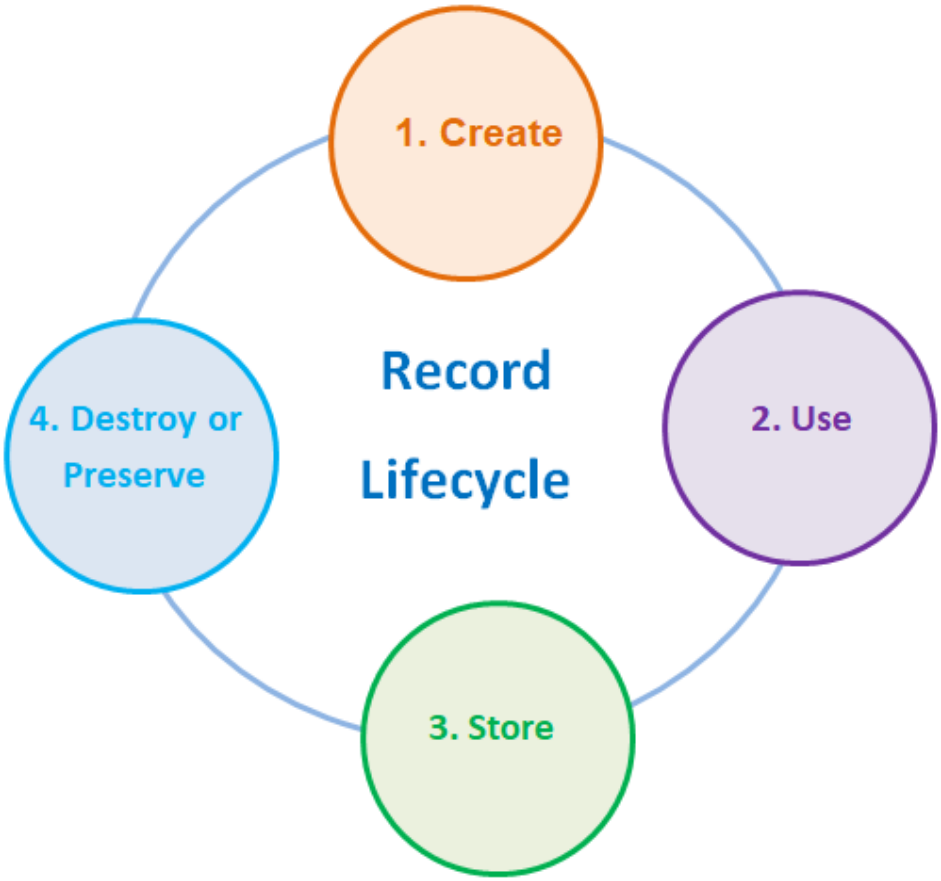
Record Management Policy

V.1



CONTENTS

DOCUMENT CONTROL

Reference	Records Management Policy V.1
Date	2021 June
Author	Victoria MacDonald
Approved	2021 September

VERSION HISTORY

Date	Version Number	Revision Notes
2021 09 30	V1	

INTRODUCTION

Records are the lifeblood of Tameside Council and the NHS Tameside and Glossop Clinical Commissioning Group (CCG). Records are the basis on which decisions are made, services provided and policies developed and communicated.

The public has a right to access information under the Freedom of Information Act 2000. These rights are diminished if information cannot be found when requested or, when found, cannot be relied upon as authoritative.

Good Records Management will benefit all staff and Service Areas in the Council and CCG. Benefits include but are not limited to:

- A reduction in time spent searching for information
- Improved information integrity due to fewer versions and duplications of documents
- Improved transparency and accountability
- A reduction in storage costs as data is cleansed
- Improved access to information
- An open and transparent foundation for decision-making
- Preservation of the Council's and CCG's corporate memory
- Supported continuity in the event of a disaster
- Enhanced customer service and improved reputation with partner organisations
- Protection and support in litigation
- Compliance with legislation and regulations such as GDPR, the Data Protection Act 1998, employment legislation and health and safety legislation
- Improved ability to demonstrate corporate responsibilities
- Business intelligence and analysis of data is reliant on excellent record keeping
- Records of value to Tameside are identified and held by the Archive

Poor Records Management creates risks for the Council and CCG, such as:

- Staff time wasted searching for information
- Inconsistent or poor levels of service
- Poor decisions based on inaccurate or incomplete information
- Financial or legal loss if information required as evidence is not available or cannot be relied upon
- Non-compliance with statutory or other regulatory requirements
- Failure to handle confidential information with an appropriate level of security
- Unauthorised access to confidential records and information, breaching GDPR regulations
- Failure to protect information that is vital to the continued functioning of the Council and CCG
- Inadequate business continuity planning
- Staff time wasted considering issues that have previously been addressed and resolved
- Unnecessary costs caused by storing records longer than they are needed
- Unauthorised disposal of records and information
- Loss of reputation as a result of all the above, with damaging effects on public trust

SCOPE AND DEFINITIONS

This policy sets out recommended good practice for the management of all records, paper and electronic, including those in dedicated Line of Business Systems.

Term	Definition
Record	Information, in any format, created or received by the Council or CCG to support and provide evidence of activities and business transactions.
Retention and disposal schedule	A document detailing how long records need to be retained before they can be destroyed.
Personal information	Information about any individual, who could be identified from the information or any other information that is in the possession of the Council or CCG. The Council and CCG are legally responsible for the storage, protection and use of all personal information held as governed by GDPR and the Data Protection Act.

SUMMARY OF RECOMMENDED GOOD PRACTICE

Good practice in records management is made of a number of key elements. Guidance on each element is given in this policy.

- Service areas clearly outline the roles, responsibilities and expectations of Records Management.
- Service areas only keep the records they need for business, regulatory, legal and accountability purposes.
- Service areas keep their records in systems that enable records to be retrieved as necessary.
- Service Areas know what records they hold and where they are, should ensure that records remain usable for as long as they are required.
- Service Areas store records securely and control access.
- Service Areas know how long they need to keep particular records; dispose records when they are no longer needed and be able to explain why records are no longer held.
- The Council and CCG ensure that records shared with other bodies or held on their behalf by other bodies are managed in accordance to this policy.

ROLES, RESPONSIBILITIES AND EXPECTATIONS OF RECORDS MANAGEMENT

Records Management is a core corporate function. Consideration of records management is needed when planning or implementing ICT systems, extending staff access to new technologies and during re-structuring or major organisation changes.

Role	Expectations
All employees, Elected Members and those individuals engaged by the Council	To manage information and create records in line with the Council's policy and procedures. All staff and individuals engaged by the Council should ensure that they are familiar with and follow any records management procedures in their service area.
Team Manager	To ensure records created by employees under their management are managed in line with the Council's policy and procedures. See appendix for tips for effective records management.
Senior Management and Chief Executive/ Accountable Officer	It is the responsibility of individual service areas to carry out and review the necessary retention and disposal requirements for their records, with advice and support from the Records Manager. The Chief Executive/Accountable Officer has senior management responsibility for records management within the Council and CCG.
Records Manager	The Records Manager has day-to-day oversight of records management within the Council and CCG. The Records Manager will: Develop policy and procedures that ensure that service areas have the ability to be compliant with policy and legislation. Provide regular training programmes for Council and CCG staff and those individuals engaged by the Council. Develop guidance and give advice to colleagues across the Council and CCG on records management issues. Provide advice on adequate storage for records and subsequent monitoring of such areas.

All Council and CCG staff will be made aware of their responsibilities and supported through regular training programmes and guidance.

The Paperless Policy advises on Line of Business Systems, electronic record storage and bulk scanning, alternatively contact ICT Services via FreshService or the ICFT (Hospital IT Team).

WHAT RECORDS NEED TO BE KEPT

Service areas need to consider what records they are likely to need, and the risks of not having those records, taking into account the following factors:

- The legislative and regulatory environment within which they operate. This will be a mixture of generally applicable legislation and specific legislation applying to the service.
- The need to refer to authoritative information about past actions and decision for current business purposes.
- The need to protect legal and other rights of the Council, CCG, staff and stakeholders.
- The need to explain, and if necessary justify, past actions in the event of an audit, public inquiry or other investigation.

All staff will be aware of which records the Council and CCG decide to retain through the Retention and Disposal Schedule.
All staff have a responsibility to keep accurate and complete records and are aware of the need to give those records titles that reflect their specific nature and contents to facilitate retrieval.
Ephemeral material can be disposed of on a routine basis, for example print outs of electronic documents, trivial emails and personal copies of documents.

DIGITAL RECORD SYSTEMS

The Council and CCG hold records on a number of different systems to meet the service area's specific needs. All record systems should have the following characteristics:

- Be easy to understand and use to reduce the effort required of those who create and use the records within them.
- Enable quick and easy retrieval of information. This should include the capacity to search for information requested under the Freedom of Information Act or Individual Rights covered by GDPR and the Data Protection Act 2018.
- Enable routine records management processes to take place. Systems should be able to delete specified information and leave the rest intact.
- Enable the context of each record, and its relationship to other records, to be understood.
- Protect records from accidental or unauthorised alteration, copying, movement or deletion.
- Provide secure storage for the level of protection required by the nature, content and value of the information in them.
- Enable an audit trail to be produced of occasions on which selected records have been seen, used, amended and deleted.

Records in digital systems will not remain usable unless precautions are taken. Corporate line of business systems and central file storage systems must be used to store all electronic records and information. ICT have strategies for continued maintenance and backup processes to ensure that information within line of business systems and central file storage systems remain intact, reliable and usable. Digital records are vulnerable to accidental or unauthorised alteration, copying and deletion which can happen without trace. This puts at risk the reliability of records which could damage the Council or CCG's interests. Service areas should assess these risks and put appropriate safeguards in place. Any information stored outside of line of business systems and central file storage systems is not maintained by ICT and is therefore vulnerable.

SCANNING RECORDS

An electronic record, scanned from the original paper record, will be accepted by a court or other legal body as long as it can be proven that it is a true copy. A clear scanning procedure will demonstrate beyond reasonable doubt that the original document had been scanned in its entirety.

All MFDs have the ability to scan and send the record to your email address or central file storage system. ICT Services can advise on specific scanning requirements such as adding workflow to records or scanning directly into line of business systems by contacting ICT Services via FreshService.

Once scanned, the paper copy can be destroyed to safeguard against duplications, ensuring that personal information is confidentially destroyed.

Important Records such as deeds, contracts, guarantees or certificates, should not be destroyed without advice from Legal Services and the express permission of those involved in the contract.

PHYSICAL STORAGE

The effectiveness of records storage depends on knowledge of what records are held, what information they contain, in what format they are accessible, what value they have to the service area and how they relate to business functions. Without this service areas will find it difficult to:

- Locate and retrieve information required for business purposes
- Locate and retrieve information required to respond to an information request
- Gather and maintain data required on the Information Asset Register
- Effectively manage the risks associated with storing records (both paper and electronic)
- Ensure records are disposed of when no longer required

Wherever possible, paper documents should be scanned and retained in an electronic format to keep the information in a readable condition and to reduce the inconvenience and cost of physical storage.

Storage for non-electronic records needs to be well organised, with all files labelled, numbered and indexed accurately. Services need to be aware of any specific requirements for records storage that apply to them.

Storage facilities need to be suitable to preserve records and protect from damage, theft and disaster (i.e. fire, water). Consideration needs to be made in regards to the future risks for non-electronic records to ensure that they remain reliable and usable for as long as required. Risks to consider include:

- The delicate nature of aging paper, including carbon paper
- The fading of pictures, photocopies and handwritten text
- Records stored on defunct technology, such as cassettes, microfiche and disks.

The whereabouts of records should be known at all times and movement of records between storage areas and office areas should be logged.

RECORDS SHARED WITH AND STORED BY EXTERNAL BODIES

When working in partnership with other organisations, sharing information and contributing to a joint records system, services should ensure that all parties agree to protocols that specify:

- What information should be kept, and by whom
- What level of information security should be applied
- Who should have access to the records
- What disposal arrangements should be in place
- Which organisation is responsible for responding to information requests

Particular protection should be given to confidential or personal information. Protocols should specify when, and under what conditions, information and records will be shared and details should be kept of when this information has been shared.

The Council and CCG are responsible for ensuring that contractors and other organisations creating records on behalf of the Council and CCG are storing and maintaining records to the standard set out in this policy. This can be done through Data Processing and Sharing Agreements, please speak to the Risk, Insurance and Information Governance team for more information.

DESTRUCTION

Children's Services Records cannot be destroyed for the foreseeable future. More information can be found in appendix 2 and 3 at the end of this policy.

The untimely disposal of documents will cause the Council or CCG:

- Difficulty in defending litigious claims
- Operational problems
- Failure in complying with Freedom of Information Requests
- Failure in complying with Subject Access Requests

Before destroying records, your service will need to consider:

- Has the record met its retention period?
- Has the record been reviewed to ensure it is no longer required?
- Is the record needed to complete a pending Freedom of Information request?
- Is the record needed to complete a pending Subject Access request?
- Have all copies, duplicates and backups been destroyed?

Where records are not destroyed as a result of review, the reasons for this action must be clearly justified. If the decision is made to extend a paper record's retention period, the record will need to be transferred to an electronic format if possible.

The method of disposal will largely depend on the format of the record. Council and CCG records must be disposed of securely using one of the following methods:

Record Format	Method of Destruction
Paper	Confidential waste bin – SHRED IT or blue locked bins in offices Shredding
Electronic	Hard deletion / scrubbing
CD	Contact IT via Freshdesk
Cassette	Contact IT via Freshdesk

Under no circumstances should records containing personal information be deposited in regular recycling or general waste bins. To do so could result in the unauthorised disclosure of such information and render the Council or CCG liable to prosecution under GDPR and the Data Protection Act.

The Council's Retention and Disposal Schedule is based on the Local Government Retention Schedule published by the Information and Records Management Society and additional sources including The National Archives and other Local Authorities. Where there are no statutory requirements to retain information, an assessment of business need has been made and some 'best-practice' time periods have been included. The schedule can be found here.

It is important that the disposal or preservation of records happen as part of a managed process and that it is adequately documented. Details of the document being disposed of; the date and method of disposal, and the officer who authorised disposal should all be recorded within the Record Review Form after answering the questions below. This is particularly important to confirm we no longer hold applicable information.

PRESERVATION

A record cannot be destroyed if it:

- Is subject to legal hold (legal proceedings)
- Contains or relates to information recently released in response to a Freedom of Information or Subject Access Request
- Is still needed by the service area; this must be supported by a legitimate business need.
- Holds historical value to the Borough of Tameside.

Council records that are no longer in use with historical value are offered to the Tameside Local Studies and Archives via the Archivist. These include meeting minutes where key decisions are made and public records.

The destruction of records subject to legal hold or recently used for a Freedom of Information or Subject Access Request will be delayed until the hold is complete or, in the case of a request for information, all relevant complaint and appeal provisions have been exhausted.
Details of the document being preserved, the business need for the record being preserved need to be recorded as part of the Record Review.

LEGISLATION AND RELATED POLICIES

This Policy has been written with reference to the Lord *Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000* which can be found on the National Archives Website.

Related Council policies include:

- IT Security Policy
- Information Governance policies
- Scanned Documents
- Paper Records Secure Handling and Transit
- Paperless Policy (not currently released)

POLICY REVIEW

This policy will be reviewed every year or when there have been any significant changes in legislation.

Appendix 1 - TIPS FOR EFFECTIVE RECORDS MANAGEMENT

Creation

Records should be created at the time of, or as soon as practicable after the event to ensure they are accurate and reliable.

Think about how you name your records and agree a format within your team or line of business system. This will make it easier to identify and retrieve documents. Top tips include:

- Keep file names short, but meaningful
- When including a number in a file name always give it as a two-digit number, i.e. 01-99, unless it is a year or another number with more than two digits.
- If using a date in the file name always state the date first and 'back to front'. Use YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY.
- When including a personal name in a file name give the family name first followed by the initials.
- Order the elements in a file name in the most appropriate way to retrieve the record.
- The file names of records relating to recurring events should include the date and a description of the event.
- The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence.
- Avoid using repetitive words such as 'draft' or 'letter' at the start of file names.
- The version number of a record should be indicated in its file name by the inclusion of 'V' followed by the version number.
- Avoid using non-alphanumeric characters in file names, for example " £ $ % ^ & * ()!
- Line of business systems often have standardised formats for file storage, contact ICT for more information.

Use

Agree a procedure within your teams as to where electronic and paper records are stored. Ensure all documents are filed in the central file storage system and not on individual desktops.

Assign responsibility for maintaining central file storage systems to a job role or member of the team.

Avoid creating duplicate or unnecessary records. Rather than email attachments to your team, save the document in your central file storage system and email a hyperlink to the team.

Avoid storing duplicate drafts of the same record. Ensure that old drafts and duplicate versions are deleted to avoid unnecessary confusion.

Discuss records management in team meetings.

Email Management

Be aware that anything you write in an email could be subject to release. Always consider the content and tone of your emails before you send them.

Delete any emails which you do not need to retain. These will include emails sent for information only, e.g. most CC emails since you are not the main recipient, outdated information or personal emails.

Check emails before you archive to ensure that you are only saving the information you need.

The retention period for all emails is 2 years. It is important to ensure any emails to be stored for retention reasons are saved in line of business or central file storage systems accordingly.

Store

Wherever possible, scan paper records and keep them electronically.

Distribute documents electronically before meetings rather than taking print outs with you, either by email or via central file storage systems. This will reduce the storage of duplicated documents. For democratic and executive meetings meeting papers are electronic through the use of modern.gov software.

End of Retention Reviews: Destroy or Preserve

Hold record clean-up days on a regular basis.

During the review consider:

- Do you need the information to carry out your business?
- Is there a legal requirement to keep the information?
- Do you need the information for financial purposes?
- Will you need the information to explain why you arrived at a particular decision?
- Will you need the information if your decision is challenged in court?
- Will you need the information to be publicly accountable for your policies and decisions?
- Will you need the information to help with similar situations in the future?
- Will you need the information to defend your rights and responsibilities, or the rights and responsibilities of others?
- Does the information have value for historical research purposes?

Appendix 2 – IICSA LETTER TO CHIEF EXECUTIVE

INDEPENDENT INQUIRY INTO CHILD SEXUAL ABUSE

Chief Executive
Local Authority
Thursday 2nd July 2015

Subject: Notice of retention/non-destruction of documents relating to the Independent Inquiry into Child Sexual Abuse

As you are aware, on 12 March 2015, the Home Secretary established the Independent Inquiry into Child Sexual Abuse to consider whether public bodies – and other non-state institutions – have taken seriously their duty of care to protect children from sexual abuse. I write to you now in my position as Chair of the Inquiry on the issue of information and records held by your organisation, and those organisations for which you are responsible, or which are affiliated to your organisation.

The Terms of Reference for the Inquiry (appended) are extremely broad. As such, it is not yet clear exactly what files, records and documents we will be requesting from your organisations. This will become clearer as the work of the Inquiry progresses. In the meantime we must ensure that no line of investigation is curtailed by the premature destruction of files or records that later become required as evidence.

Accordingly, I have set out in an appendix to this letter a list of categories of document that should be retained pending further requests from the Inquiry. I would be grateful if you could ensure a thorough search of all your paper files, all digital records, and all other information – however held – to ensure that everything of potential relevance to the Inquiry is retained.

Please circulate this letter and its appendices to all parts of your organisation, to those bodies for which you are responsible, or which are affiliated to your organisation. **It is of particular importance that your Children's Services Department and designated officer, or team of officers, (as described in the statutory guidance: Working Together to Safeguard Children March 2015) receive and act upon this request.**

I thank you for your continued assistance in this matter.

Yours sincerely

Lowell Goddard
Chair, Independent Inquiry into Child Sexual Abuse

Appendix 1: Categories of document for retention

Your organisation is asked to retain any and all documents; correspondence; notes; emails and all other information – however held – which contain or may contain content pertaining directly or indirectly to the sexual abuse of children or to child protection and care. For the purposes of this appendix, the word "children" relates to any person under the age of 18.

Such information may include, but is not limited to, the following:

a. Any material, including reports; reviews; briefings; minutes; notes and correspondence in relation to allegations (substantiated or not) of individuals, organisations, institutions, public bodies or otherwise who may have been involved in, or have knowledge of, child sexual abuse, or child sexual exploitation;

b. Any material, including reports; reviews; briefings; minutes; notes and correspondence in relation to allegations (substantiated or not) of individuals having engaged in sexual activity with, or having a sexual interest in, children;

c. Any material, including reports; reviews; briefings; minutes; notes and correspondence in relation to institutional failures to protect children from sexual abuse or other exploitation;

d. Any material relevant to statutory responsibilities for the care of children in public or private care;

e. Any material relevant to the development of policy on child protection;

f. Any material relevant to the development of legislation on child protection;

g. Any material relating to the determination of the award of Honours to persons who are now demonstrated to have had a sexual interest in children or are suspected of having had such an interest.

It is not possible to produce a definitive list under (g). Accordingly we invite you to ensure that no documentation relating to the award of Honours to any person is destroyed pending the outcome of the Independent Inquiry.

Appendix 2: Terms of reference

Terms of Reference

Purpose

1. To consider the extent to which State and non-State institutions have failed in their duty of care to protect children from sexual abuse and exploitation; to consider the extent to which those failings have since been addressed; to identify further action needed to address any failings identified; to consider the steps which it is necessary for State and non-State institutions to take in order to protect children from such abuse in future; and to publish a report with recommendations.

2. In doing so to:
   a. Consider all the information which is available from the various published and unpublished reviews, court cases, and investigations which have so far concluded;
   b. Consider the experience of survivors of child sexual abuse; providing opportunities for them to bear witness to the Inquiry, having regard to the need to provide appropriate support in doing so;

c. Consider whether State and non-State institutions failed to identify such abuse and/or whether there was otherwise an inappropriate institutional response to allegations of child sexual abuse and/or whether there were ineffective child protection procedures in place;
d. Advise on any further action needed to address any institutional protection gaps within current child protection systems on the basis of the findings and lessons learnt from this inquiry;
e. Disclose, where appropriate and in line with security and data protection protocols, any documents which were considered as part of the inquiry;
f. Liaise with ongoing inquiries, including those currently being conducted in Northern Ireland and Scotland, with a view to (a) ensuring that relevant information is shared, and (b) identifying any State or non-State institutions with child protection obligations that currently fall outside the scope of the present Inquiry and those being conducted in the devolved jurisdictions;
g. Produce regular reports, and an interim report by the end of 2018; and
h. Conduct the work of the Inquiry as transparent a manner as possible, consistent with the effective investigation of the matters falling within the terms of reference, and having regard to all the relevant duties of confidentiality.

Scope

3. State and non-State institutions. Such institutions will, for example, include:
    a. Government departments, the Cabinet Office, Parliament and Ministers;
    b. Police, prosecuting authorities, schools including private and state-funded boarding and day schools, specialist education (such as music tuition), Local Authorities (including care homes and children's services), health services, and prisons/secure estates;
    c. Churches and other religious denominations and organisations;
    d. Political Parties; and
    e. The Armed Services.
4. The Inquiry will cover England and Wales. Should the Inquiry identify any material relating to the devolved administrations, it will be passed to the relevant authorities;
5. The Inquiry will not address allegations relating to events in the Overseas Territories or Crown Dependencies. However, any such allegations received by the Inquiry will be referred to the relevant law enforcement bodies in those jurisdictions;
6. For the purposes of this Inquiry "child" means anyone under the age of 18. However, the panel will consider abuse of individuals over the age of 18, if that abuse started when the individual was a minor.

Principles

7. The Inquiry will have full access to all the material it seeks.
8. Any allegation of child abuse received by the Inquiry will be referred to the Police;
9. All personal and sensitive information will be appropriately protected; and will be made available only to those who need to see it; and
10. It is not part of the Inquiry's function to determine civil or criminal liability of named individuals or organisations. This should not, however, inhibit the Inquiry from reaching findings of fact relevant to its terms of reference.

The original document can be found here [Microsoft Word - Generic Letter to LA CEO v2.docx (iicsa.org.uk)]

Appendix 3 –IICSA GUIDANCE NOTE REGARDING RETENTION

INDEPENDENT INQUIRY
CHILD SEXUAL ABUSE

Guidance Note: Retention Instructions and Data Protection requirements (version 2)

The Inquiry has issued retention instructions to a range of institutions requesting the preservation of all records relating to the care of children so that they remain available for inspection by the Inquiry. Justice Goddard also stated in her opening statement on 9 July 2015 that *"No institution – whether they have received a letter or not – can be in any doubt of the extent of their duty to preserve records for the Inquiry, or of the consequences of failing to do so"* (paragraph 77).

The Inquiry received a number of queries about the possibility that prolonged retention of personal data in accordance with the retention instructions might engage issues of compliance with data protection legislation. The Inquiry consulted with the Information Commissioner's Office and, having done so, issues this Guidance to clarify the position.

Under Section 21 of the Inquiries Act 2005 the Inquiry has the power to order the production of documents. Failure to comply with such an order without reasonable excuse is an offence punishable by imprisonment (Section 35 of the Inquiries Act 2005). It is also an offence for a person, during the course of an Inquiry, to destroy, alter or tamper with evidence that may be relevant to an Inquiry, or deliberately to do an act with the intention of suppressing evidence or preventing it being disclosed to the Inquiry.

Institutions therefore have an obligation to preserve records for the Inquiry for as long as necessary to assist the Inquiry. Prolonged retention of personal data by an organisation at the request of the Inquiry would not therefore contravene data protection legislation, provided such information is restricted to that necessary to fulfil any potential legal duties that organisation may have in relation to the Inquiry. An institution may have to account for its previous activities to the Inquiry so retention of the data will be regarded as necessary for this purpose.

The obligation to the Inquiry to retain documents will remain throughout its duration. Institutions may also incur separate legal obligations to retain documents during the course of the Inquiry, for example in relation to other legal proceedings.
25 July 2018

The original document can be found here 2018-07-25-guidance-note-retention-instructions-data-protection-requirements-version-2.pdf (iicsa.org.uk)

Appendix 4 –RECORD REVIEW FORM

Record Review

Please read the questions below to ensure that records are not being disposed of prematurely. Send a copy of the completed Record Review Form to the Records Manager.

Date of Review	Description of records	Type of records	Storage location	Destruction confirmed or retention extended	Reason for extending retention	Next review date	Destruction date	Authorised by (name)	Authorised by (job role)
01/01/2021	*example box A*	*paper*	*Tameside One floor 4*	*destruction*			*02/01/2021*	*A Example*	*Records Manager*
01/01/2021	*example file B*	*electronic*	*shared file*	*retention extended*	*subject to FOI request*	*01/10/2021*		*A Example*	*Records Manager*

Record Review Questions

- Do you need the information to carry out your business?
- Is there a legal requirement to keep the information?
- Do you need the information for financial purposes?
- Will you need the information to explain why you arrived at a particular decision?
- Will you need the information if your decision is challenged in court?
- Will you need the information to be publicly accountable for your policies and decisions?
- Will you need the information to help with similar situations in the future?
- Will you need the information to defend your rights and responsibilities, or the rights and responsibilities of others?
- Does the information have value for historical research purposes?

If you have answered yes to any of the above questions, the record should be retained . Outline the reason for, and length of retention on the Record Review Form above.