HANDBOOK ON JUDICIAL INFORMATION MANAGEMENT

Section 1: Core principles

Section 2: Relevant Stakeholders for data exchanges in the Justice System

Section 3 : Enforcement mechanism

Section 4: Draft Judicial Information Management Policy

a. Part I - Definitions
b. Part II- Policy on Collection, Processing, Retention, Storage and Deletion
c. Part III - Policy on Access to Court Records
d. Part IV- Policy on Complaints Handling
e. Part V - Miscellaneous
f. Schedules (Storage and retention timelines, Access Matrix, Application for Bulk access, Compiled information and extended access, Privacy Notice, Forms under complaints handling)

Section 5: Practice Notes for Court Staff and Judges [Work in Progress]

Section 6: FAQs for Citizens and Litigants [Work in Progress]

Section 7: Pilot Projects

SECTION 1: CORE PRINCIPLES

Courts in India are familiar with the constitutionally mandated and statutorily recognized principle of open courts. Under Article 145(4) of the Constitution, the Supreme Court is required to issue its judgments only in open courts. This principle is further buttressed by provisions within the Civil Procedure Code, 1908 and the Criminal Procedure Code, 1973 which require hearings in civil and criminal cases by subordinate courts within open courts that allow for public attendance.[1] A nine-judge bench of the Supreme Court, in *Naresh Shridhar Mirajkar v. State of Maharashtra*, has stated that a court of justice is a public forum, and that apart from rare and exceptional cases, trials must be open to all and reporting of court proceedings must not be restrained in the interests of the public's confidence in the judiciary.[2]Open courts serve the purpose of allowing courts to be more accessible to the public, and to ensure that '*justice is not only done, but is also seen to be done*'- a key aspect of ensuring faith in the judiciary.

A key component of the principle of open courts is permitting public access to certain court records. Judgements and orders emanating from a case, for example, are always matters of public record and accessible to the general public, through which the public may understand the rationale for a verdict as given by the judge hearing a case. Further, additional sets of data which are presented to the records of the court, or are generated by the court, have also been included with the ambit of access to public records.

However, the principle of public access to records must be balanced with the concerns of breach of privacy owing to the vast amounts of personally identifiable information processed by courts across India. Further, the digitisation of court records, while increasing accessibility and efficiency of courts, raises the concern of misuse and harm towards the participants of the judicial system in the event of such personal information being wrongly accessed or disclosed. Accordingly, this Handbook seeks to set out a framework for access based on the various types of stakeholders within the judiciary, with demarcations on the kind of information to be accessible to each set of stakeholders.

In India, *Justice K.S. Puttaswamy and another* v. *Union of India*[3] (**Puttaswamy I**) recognised the right to privacy as an intrinsic part of right to life and liberty under article 21 and right to freedom of speech and expression under Article 19. *Puttaswamy I* considered the three essential facets of privacy to be "repose" i.e. freedom from unwanted stimuli, "sanctuary" i.e. protection against intrusive observation and "intimate decision" i.e. decisional autonomy with respect to personal life choices.[4] While the right to data protection and privacy have been recognised as distinct in other jurisdictions,[5]

---

[1] Section 153B of the Code of Civil Procedure, 1908 (CPC) holds that the place of trial is to generally be an open court which is to be accessible to the public to the extent that it can accommodate them, unless the judge sees fit to revoke public access. Order 18, Rule 4 of the CPC requires witness statements to be taken in open court under the supervision of a judge. Further, under section 327 of the Code of Criminal Procedure, 1973 (CrPC), the place of inquiry or trial in criminal cases is to be an open court, to the extent it can accommodate public attendance. Judgment is to be pronounced in an open court under s. 265F. Additionally, the evidence of witnesses is to be taken in an open court under s. 274, 275, and 276 of the CrPC.

[2] Naresh Shridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1, para 143, 144

[3] Justice K.S. Puttaswamy and another v. Union of India, (2017) 10 SCC 1.

[4] Para 36, Justice K.S. Puttaswamy and another v. Union of India, (2017) 10 SCC 1 (Kaul J.)

[5] Daksh, Judicial Data Regulation Discussion Paper I: Balancing Open Courts with the Right to Privacy - An Indian Perspective, June 2021 available at https://dakshindia.org/wp-content/uploads/2021/06/DAKSH-Paper-I-Balancing-Open-Courts-and-the-Right-to-Privacy-An-Indian-perspective-2021-06-23.pdf.

the right to data protection in the Indian context could be understood to be drawn from the right to privacy to the extent that *Puttaswamy I* emphasizes on autonomy of an individual.[6] However, like other rights, the right to privacy and data protection is not absolute, and would be hemmed in by reasonable restrictions.

Keeping the foregoing principles in mind, the Handbook seeks to balance the concerns of data protection and privacy vis-à-vis judicial records with the need to ensure optimal use of technology to promote public access to records. This balancing of interests is sought to be done by creating a three-fold system to ensure personal data protection while providing for a mechanism for access to court records data in a tiered structure.

A.Data Processing and Data Retention:

The Judicial Information Management Policy (**'the Policy**') pertaining to personal data in judicial records seeks to ensure that personal data processed by courts does not fall foul of concerns of over-collection, function creep, and is proportional to the purposes for which it was collected. It does so by incorporating data protection concepts of collection limitation, purpose limitation and rights of data subjects in the Policy. Put simply, collection limitation requires that only such data be collected as is required for the specific purpose of processing, while purpose limitation requires that data should be processed only for such purposes as it was collected for.

In implementing some of these concepts, a distinction needs to be made between data that is collected for judicial decision making and data collected for administrative purposes in aid of such judicial decision making. This stems from the relative difference in the scope of powers of data collection between the two. The Court draws its powers to call for information from various statutes. Providing limitations on such powers, would first, be legally untenable and second, impact judicial independence. Therefore, the Policy, primarily, applies the concept of collection limitation to the administrative functions of the judiciary. In doing so, it specifies the fields of information that may be collected for registration of a case and the verification of such information. In so far as purpose limitation is concerned, the Policy provides that the data is processed only for purposes mentioned therein. The Policy also provides the data subjects with the rights of notice, access, confirmation and correction of their data. While the right to notice applies to both collection of data both for judicial decision making and other functions, the rest of the rights apply only to non-judicial decision making functions.

Additionally, the Policy requires the deletion of personal data for court records maintained both in the digitised or physical form in line with the applicable timelines for each court prescribed in court rules framed under the Destruction of Records Act, 1915. The timeline for deletion has been framed this way to avoid a duplicity of storage and deletion timelines between physical and digitised files by each High Court and its respective subordinate courts, or to prematurely remove personal data references from records while they are in storage, affecting the interests of justice in the event of reopening the case records. Further, the Policy seeks to provide a timeline for the storage and deletion of data collected in the course of the eCourts project, by imposing timelines on deletion of user-submitted

[6] Para 177, Justice K.S. Puttaswamy and another v. Union of India, (2017) 10 SCC 1 (Chandrachud J.)

data and automatically collected data from the eCourts web portal and the eCourts Services mobile application.

B.Access:

The Policy prescribes a tiered system of access to various types of judicial data to various stakeholders in the judicial system, which includes litigants, parties relevant to ongoing cases, representatives from appropriate government, and the general public. Part III of the Policy seeks to set out the types of information for which an open access system is envisioned, and the datasets that have restricted access for specific user groups built in. In this regard, open access information has been classified as information that comprises of judgments, directions and orders issued by the court, records of the act of the court, [transcripts of proceedings in open courts, pleadings made by parties submitted to the court after the disposal of a particular matter,] and additional datasets that may be prescribed as open access documents. All other information processed or generated by the courts comprises the restricted access documents, the access to specific documents within which has been provided to specified stakeholders.

The use of modern technology for bulk access to digitized court documents has been recognized in a framework that discusses bulk access of judicial records in specific instances for restricted access items and more generally for open access documents. Bulk access is generally sought to be provided for open access documents, as such documents are a matter of public record. Bulk access for restricted records, on the other hand, may be provided in certain specific purposes such as scholarly, journalistic, governmental, research, evaluation or statistical purposes where the identification of specific individuals is ancillary to the purpose of the inquiry. However, to guard against possible misuses of bulk access to personal data that may be present within restricted access documents, the Policy proscribes any access to restricted access information towards use-case scenarios such as direct or indirect commercial activities that involve providing such information to the public, unlawful surveillance, profiling, or unlawful discrimination.

C.Grievance Redressal:

This Handbook seeks to serve as model guidelines to be implemented and enforced at each level of the judiciary, and accordingly the Policy includes a model grievance redressal framework. This framework provides the stakeholders of the judiciary with a mechanism to seek remedies for contravention to these policies. The grievance redressal mechanism for the Supreme Court and each High Court shall include a designated person to increase awareness of, and to ensure compliance with, the provisions of the Policy. Further, data principals seeking certain specified reliefs or the compliance officer, noting a non-compliance of the Policy shall address their representations to a designated grievance redressal officer. Finally, any review of the decisions taken by the grievance redressal officer shall be conducted by a designated three-member committee appointed by the respective Chief Justice of that court. This framework seeks to allow for grievances raised regarding violations of the Policy and certain additional reliefs that may be sought by data principals to be addressed within the prescribed timelines.

The e-Courts project, providing greater accessibility and embracing new technologies, must go hand in hand with the principles of open courts and access to public records, balanced with the principle of personal data protection from misuse or harm to the stakeholders of the judicial system in India. The Policy has been drafted keeping these goals in mind.

SECTION 2: RELEVANT STAKEHOLDERS FOR DATA EXCHANGES IN THE JUSTICE SYSTEM

1. Viewing the system as a whole:

Strengthening the rule of law cannot be successful without considering different perspectives and viewing the system as a whole. Consulting with a range of stakeholders is essential for achieving effective and lasting reform. Stakeholders are organizations, interest groups and individuals with a role or interest in the justice system, including within informal structures. Keeping in mind the perspectives of the users of the legal system, the Judicial Information Management Policy ('the Policy') has been formulated to ensure access and protection for all sections of society. Issues specific to each of these stakeholders need to be addressed. Optimum coordination and cooperation among various stakeholders of the judiciary is the key in bringing efficiency and fairness.

2. Stakeholder Groups:

Within the context of judicial proceedings, it is useful to consider a judicial information management system that caters to broadly three stakeholder groups:

2.1 Internal, meaning those individuals and agencies within the justice system like investigation and law enforcement agencies, prosecution, judges, registry and other court staff, the Bar and lawyers, prison officials, vendors who provide technological or other type of services to the judiciary etc;

2.2 External, meaning those actors (e.g., the accused, convicted offenders, plaintiffs, defendants, witnesses, or victims) who have a relationship with the justice system but are not an operational part of the system; and

2.3 Public, meaning individuals or groups with no relationship or participation in proceedings, which would include citizens, civil society, journalists, academic researchers, and entities in the emerging legal tech industry.

2.4 The table below summarizes at a high level the judicial data needs of key stakeholders and the purposes for which such data is required.

Stakeholder Category	**This group includes:**	**Purpose**
Judiciary	Judges, Registry, Court Staff, Court appointed officers like receivers, liquidators	Judges, Registry and other court staff require greater access than the public does to perform their official duties and carry out their responsibilities effectively. For example, judges performing judicial functions require access to all information including personal and sensitive personal information to decide a case fairly whereas access to such personal information may not be relevant for the public.

Stakeholder Category	This group includes:	Purpose
		Courts should adopt an internal policy regarding use of information in court records by judges and different categories of court staff, including the need to protect the confidentiality of information in court records. For example, the Registry is responsible for day to day administration of the court. For systematic functioning and efficient disposal of work, the Registry is generally divided into two main wings, viz. administration and judicial, which are further divided into various divisions, branches, sections and cells. The subject matters dealt with by each and every section are well defined. The different sections of the Registry must only access those information/data points that are relevant to carrying out the functions entrusted to their sections.
Court users	Litigants, Accused, Victims, Witnesses and Experts, their Lawyers	Court users are generally entitled to complete access to information in their own case as they have a legitimate interest in the outcome of the court proceeding by virtue of their direct participation in it. But such court users do not always have a legitimate interest in seeking a higher level of access than members of the general public to information in other cases in which they are not a participant.
Legal professionals	Lawyers and Advocates, Bar Associations, Public Prosecutors, Legal-aid and Pro-bono lawyers	Enabling free access to case laws, transcripts and other forms of judicial data will help legal professionals, especially smaller firms and young lawyers who cannot afford subscriptions to private legal publishers, in their legal research and preparation and thereby enable them to provide effective legal aid and support to their clients. It will also help legal aid/ support organizations for prioritizing resources and designing services.
Justice System Partners	Investigation agencies, Law Enforcement agencies, Prison Officials, Probation Officers, Child Welfare Committee, District Child Protection Unit and Special Juvenile Police Unit	These institutions are often required to process personal data for the purpose of investigating suspected crimes, for maintaining law and order situation and ensuring public safety.
Executive Branch	Ministries, departments and	As the executive branch is tasked with implementing the law and delivering critical services to the judiciary

Stakeholder Category	This group includes:	Purpose
	offices of different levels of government	(finances, infrastructure etc.), exchange of judicial data between them can improve policy making and the administration of justice. However, the executive branch cannot have unlimited access to all kinds of judicial data without any legitimate interest unless it shows how such data is useful for it to perform its constitutional, legal and official duties.
Legislative Branch, Constitutional and Statutory Bodies	Parliament, State legislatures, Legislative Committees, Task forces/ Commissions	Judicial data, especially aggregates and statistics, can improve early identification of legislative issues affecting the administration of justice and thereby enable legislative bodies to evaluate reforms and develop further laws to support policy aims in relation to the judiciary.
Suppliers	Vendors, Contractors, Service Providers (IT and other services)	Vendors, contractors and other entities, and their employees and subcontractors, who provide services to the court i.e. when court services that have been "outsourced", may also need greater access to information to do their jobs. For example, it is a common situation where information technology services are provided to a court by another agency, usually in the executive branch, or by outsourcing of court information technology services to non-governmental entities who are then provided access to information which may not be available to the public. The Court is the custodian of its records and court records are under the control of the judiciary, irrespective of the fact that such information may be maintained in systems that are not operated directly by the judiciary. Therefore, regulating vendors, contractors, suppliers and other third-party entities accessing court records is particularly relevant to the issue of liability of the court for unauthorized release of court records or information that causes harm. Therefore, in the contract for service, bulk access and other forms of extended access, Courts must consider including provisions such as requiring regular updates of the information in the third party's database to match the official court records, establishing a process for monitoring the third party's compliance with conditions imposed by the Court and check its record for providing appropriate access and protecting restricted information.
Legal sector experts	Educational institutions,	Access to judicial data for research purposes, oftentimes in excess of what is available to members of the general

Stakeholder Category	This group includes:	Purpose
	Academics, Researchers, NGOs and think-tanks	public, is necessary to understand the systemic impacts of the functioning of the justice system, for example, whether certain demographic characteristics contribute to what happens in the court. It would facilitate the linkage of judicial data to other data sets (like health, finance, education) so that researchers could better understand the antecedents of justice problems – providing a basis for upstream interventions to prevent their emergence.
Media	Journalists, Broadcasters	Even though court proceedings are generally open to the public, relatively few members of the public have used that open door. Instead, court reporters, journalists and both print as well as broadcast media have served as the intermediary between the justice system and the wider community. The media performs an important and constitutionally protected role (right to freedom of expression) as the public's watchdog over judiciary by informing and educating them about what goes on in the courtroom. It plays an indispensable role in the effective realization of the principle of open justice.
Businesses	Law-tech/Legal-tech entities, Publishers, Aggregators and Distributors	Many third-party entities seek bulk access to court records, access to judicial statistics, aggregates and compiled information in order to design tools, software, products and databases that facilitate access to justice and improve the efficiency of judicial process through technological innovation. In this context, judicial data is a two-way street. Technology can help us derive useful insights from judicial data, and judicial data can drive technologies that will help us schedule and plan judicial processes more effectively. As the Court has the ultimate responsibility for safekeeping its records, it must strictly regulate access to judicial data for commercial purposes.
Public	Members of general public	Public access to judicial data bolsters several democratic values — the right to know the law and to understand its application, permitting citizens to observe and evaluate the operation of the different branches of government including the judiciary, and a repugnance for arbitrary power. By understanding their legal rights and obligations, members of the public can effectively defend their claims, evaluate the legal advice and services tendered to them by legal professionals, and

Stakeholder Category	This group includes:	Purpose
		can seek accountability from the judicial system.

3. Judicial Information Management must account for role, function, interaction and relationship of various stakeholders with the justice system

3.1 The Policy is mindful of the various types of interactions that different individuals and groups have with the courts, and how their personal information is collected and intended to be used in the judicial process. For example, a convicted criminal's personal information would be dealt with differently than a witness's personal information. Witnesses need to have the confidence to come forward to assist law enforcement and prosecutorial authorities and therefore may be afforded greater degree of privacy protection with regard to their personal information than a person who has been convicted of a crime. However, this does not mean that a convicted person completely loses his right to privacy. As has been held by the Supreme Court of India in several instances, the protection of Article 21 (and therefore the right to privacy) is available even to convicts. Furthermore, treatment of personal information collected for investigation may differ from information collected and used in a case processing system.

3.2 One must note that when considering the "internal" audience, there is a tendency to assume a free flow of personal information relating to anyone with a "relationship" to the justice system, as long as the sharing is done for stated and lawful purposes. Existing rules for sharing information within the criminal justice system (e.g., police, prosecutors, defence, courts, and prisons) would differ from rules used to determine the disclosure of that information to parties outside the justice system. For example, evidence collected by police or investigation agencies would need to be shared with public prosecutors, the accused, and their lawyer; but these are generally not made public. Even among external actors, multiple groups play a vital role in maintaining accountability of the judiciary and other public institutions, such as journalists and civil society organizations.

3.3 Increasingly, justice agencies are working together to plan, design, and implement integrated justice information sharing systems. These systems enhance the ability to collect, access, and use information, including personal information, and allow information to be entered once and used across and between many different agency systems. For example, the Crime and Criminal Tracking Network & Systems (CCTNS), a Mission Mode Project under the National e-Governance Plan (NeGP) of the Government of India aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals'. This will necessarily entail exchange of data between the police, courts and the government. There is a need to address data security and privacy issues during the planning stages of the information management systems of such integrated justice systems. Implementation without privacy planning can result in having to manage unintended privacy effects and having to retool the system to address these effects. Efforts should also be made to inform the various stakeholders of what kinds of information, including their personal information, are shared with the different agencies within the integrated justice information sharing systems.

SECTION 3: ENFORCEMENT MECHANISM

To ensure the realisation of the substantive rights recognised and procedures laid out in Parts II & III of the Policy, Part IV provides for complaints handling mechanism recognising that a policy is only as good as its enforcement.

Part IV is based on a review of regulations adopted by comparative jurisdictions, academic literature, existing laws and the practice of courts in implementing rules. It has twin goals - **1)** ensure *ex-ante* compliance of the Policy by sensitising stakeholders and monitoring data processing practices, and **2)** establish a procedure to redress grievances against non-compliance with the Policy.

At the apex of the complaints handling mechanism is a committee to handle grievances arising from non-compliance with the Policy ('**the Committee**'). Along with the Committee, Part IV of the Policy contemplates a Compliance Officer and a Grievance Redressal Officer, both of whom must have experience in the field of Information Technology. The functions of the Committee (**A)**, the Compliance Officer (**B)** and the Grievance Redressal Officer (**C**) are detailed in the paragraphs below. The paragraphs below also detail the procedure to institute representations regarding non-compliance with the Policy (**D**).

A. Committee for handling complaints regarding Judicial Information Management Policy

a. **Independence of Judiciary:** The Committee will be constituted by the Hon'ble Chief Justice of High Court of *Judicature* to handle complaints arising from the Policy. Thus, Part IV of the Policy provides for the judiciary to itself resolve complaints arising out of data processed by the courts. This is consistent with the principle of independence of the judiciary which has been recognised as part of the basic structure of the Constitution by the Hon'ble Supreme Court in *Advocate on Record Association vs Union of India,* 1993 (4) SCC 441.

b. **Constitution of the Committee:** The Committee shall consist of a chairperson and two members, chosen from among the judges of the High Court. The term of the Committee shall be subject to the discretion of the Chief Justice. The constitution of the Committee is modeled after similar committees which have been constituted by High Courts across the country. For example, the Delhi High Court has committees that adjudicate complaints related to - unauthorised construction in court complexes, the appointments of Law Researchers/Law Interns, and issues of sexual harassment (Prevention of Sexual Harassment Act, 2013). The European General Court also provides for a similar committee to adjudicate complaints related to the processing of personal data by the General Court.

c. **Assistance to the Committee:** Part IV of the Policy enables the Committee to invite technical members, and members from the Bar to assist the Committee in handling complaints related to the Policy. Clause 2(f) provides that the technical members and members from the Bar shall not exercise decision-making powers, and maintain confidentiality regarding the proceedings of the Committee.

B. Responsibilities of the Compliance Officer

a. **Ensure compliance with the Policy:** Part IV of the Policy provides for a Compliance Officer to ensure the Policy is complied with in letter and spirit. To that end, the Compliance Officer is responsible for auditing data processing practices within the High Court of *Judicature* as well as the practices of the lower judiciary.

b. **Address representation to the Grievance Redressal Officer:** In case the Compliance Officer while auditing data processing practices of courts or otherwise, finds non-compliance

with the Policy, they can address a representation to the Grievance Redressal Officer who will pass appropriate orders.

c. **Sensitise the courts & the public regarding the Policy:** Since this is an evolving field of law, the Compliance Officer has the responsibility of sensitising the judiciary, the registry and the public at large regarding the rights, obligations and responsibilities provided by the Policy. The need to sensitise stakeholders has been recognised in the Judicial Data Regulation Discussion Paper - II published by DAKSH and also the Terms of Reference of the Judicial Data Protection Panel of England & Wales. One of the mechanisms by which the Compliance Officer will ensure sensitisation is by publishing a document consisting of Frequently Asked Questions on the High Court's website and is updated from time to time. An example of an FAQ that may be uploaded on the High Court website is available here. The Compliance Officer shall also ensure that the policy is physically displayed in the High Court of *judiciature* and subordinate judiciary.

C. Responsibilities of the Grievance Redressal Officer:

a. **Address representation regarding non-compliance of the Policy:** The Grievance Redressal Officer shall address representations against non-compliance with the Policy including those raised by the Compliance Officer. Part IV of the Policy provides that any decision of the Grievance Redressal Officer may be reviewed by the Data Principle or their representative before the Committee. Thus, the Office of the Grievance Redressal Officer has been provided to act as a gatekeeper to the Committee. This ensures that the Committee is not flooded with complaints and grievances that do not require the application of judicial mind are resolved by the Office of the Grievance Redressal Officer.

b. **Refer to the Committee:** The Grievance Redressal Officer has been directed to refer to the Committee any representation seeking erasure or redaction of personal data or processing of personal data. Such requests require the application of the judicial mind as they may involve a question of law.

c. **Process requests regarding access of Personal Data:** The Grievance Redressal Officer shall also process any requests from the Data Principal seeking a copy of personal data or a confirmation of the processing of personal data. The Grievance Redressal Officer may charge a reasonable fee to provide a copy in case Data Principal's Personal Data is found to be excessive. This is consistent with Article 12 read with Article 15 of the General Data Protection Regulation of the European Union.

D. The procedure provided in the Part IV of the Policy

a. **First Instance:** A Data Principal aggrieved by non-compliance with the Judicial Information Management Policy may address a representation to the Grievance Redressal Officer. The Data Principal must make the representation by filing a form provided in Schedule I to Part IV of the Policy.

b. **Responsibility of the Grievance Redressal Officer:** The Grievance Redressal Officer must acknowledge the receipt of the representation within a period of 7 days and shall refer to the Committee any representation seeking withdrawal of consent to process data or asking for personal data to be erased or redacted or challenging the processing of personal data within 7 days from the date of acknowledging the receipt of the representation. The Committee, in turn, has the decision to grant or refuse to grant the relief sought by the Data Principal.

c. **Decision making power of the Grievance Redressal Officer:** In case of representations that are not referred to the Committee, the Grievance Redressal Officer shall decide upon the representations made by the Data Principal or the Compliance Officer within a period of 60

days. The decision of the Grievance Redressal Officer must be a reasoned order in writing, must be made available to the Data Principals.

d. **Review by the Committee:** Part IV of the Policy enables Data Principals to approach the Committee regarding decisions taken by the Grievance Redressal Officer or if the Grievance Redressal Officer does not decide a representation within a period of 60 days. The review must be preferred within a period of 14 days of the decision of the Grievance Redressal Officer, and the Committee may annul, vary or uphold the decision of the Grievance Redressal Officer.

e. **Decision subject to the approval of the Chief Justice:** The Chief Justice of the High Court of *Judicature* is the administrative in-charge of the High Court. As such, in accordance with settled practice, each decision of the Committee and of the Grievance Redressal will be subject to approval by the Chief Justice.

f. **Timelines**: The timelines provided in Part IV of the Policy are indicative in nature.The timelines should be subject to the discretion of the High Courts. Each High Court may want to provide a different time period to address representation/complaints based on the workload of their judicial officers.

SECTION 4: POLICY ON JUDICIAL INFORMATION MANAGEMENT

Part I:
Definitions

Clause 1:

1. **'Access'** includes, at the minimum, the right to view a Court Record. The Court may use its discretion to expand or limit Access to include the right to obtain copies, disseminate or use the Court Record in a particular manner, depending on the user role, jurisdiction, case type, type of Court Record or other factors that it considers relevant.

2. **'Administrative purposes required for the discharge of judicial function'** shall include functions related to the management of the data by the judicial officer for the purposes of assisting the court in its judicial decision-making functions and shall include:
   (a)filing of cases in the respective court;
   (b)issuance and service of legal processes;
   (c)file tracking and maintenance of judicial records;
   (d)preparation and timely issuance of cause lists; and
   (e) any other functions that may be determined by the Court

3. **'Bulk Access/ distribution'** of court records means access to all, or a significant subset of court records in electronic and machine readable form, without any form of compilation or aggregation.

4. **'Committee'** means the committee constituted by the Hon'ble Chief Justice under Rule 2 to handle complaints arising under these rules

5. **'Compiled Information'** is the information that is derived from the selection, aggregation or reformulation by the court of some of the information from more than one individual court record.

6. **'Compliance Officer'** means the officer of the High Court of *Judicature* appointed by the Chief Justice to be responsible for implementing this Policy.

7. **'Court'** shall mean the relevant court in India in which this Policy has been adopted, and shall include the Supreme Court of India, the High Courts, district courts, and other subordinate courts, but shall not refer to tribunals or other quasi-judicial bodies.'High Court'means High Court of *Judicature*, including all its benches.

8. **(1) 'Court Record(s)'** includes:

   (a)Any document, information, or other thing, either in a paper format or in electronic form, that is collected, received, or maintained by a court or clerk of court in connection with a judicial proceeding, which could include electronic evidence, party pleadings, affidavits, submissions, notices and responses, and

all other documents generated, received or stored by the Court in the process of a judicial proceeding.

(b)Any index, calendar, docket, register of actions, official record of the proceedings, order, decree, judgment, minute, and any information in a case management system created by or prepared by the court or clerk of court that is related to a judicial proceeding; and

(c)The information maintained by the court or clerk of court pertaining to the administration of the court or clerk of court office and not associated with any particular case, which may include returns, personal files of court staff, correspondence, and account books maintained for that court.

(2) 'Court Record' does not include:

(a)Other records maintained by the public official who also serves as clerk of court.[Court should identify and list non-court records, for example: land title records, birth records, naturalization records and voter records etc];

(b)Information gathered, maintained or stored by a governmental agency or other entity to which the court has access but which is not part of the court record as defined in Clause 1.8(1).

9. **'Data'** shall mean a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

10. **'Data Principal'** means the natural person to whom the personal data relates.

11. '**Digital Preservation SOP**'shall refer to the Digital Preservation Standard Operating Procedure published by the E-Committee, Supreme Court of India on 24 September 2021, and shall any include references to any document that amends, edes or replaces that document

12. **'Electronic Form'** - Information in a Court Record "in electronic form" includes information that exists as:

(a) electronic representations of text or graphic documents;

(b) an electronic image, including a video image, of a document, exhibit or other thing;

(c) in the fields or files of an electronic database;

(d) an audio or video recording, analog or digital, of an event or notes in an electronic file from which a transcript of an event can be prepared.

13. **'Grievance Redressal Officer'** means the officer of the High Court of *Judicature* appointed by the Chief Justice who will be responsible for addressing grievances raised against non-compliance of the Policy.

14. **'High Court'** means High Court of *Judicature*, including all its benches.

15. **'Judicial decision making'** shall mean the process of making a judicial determination on any point of law or fact.

16. **'Open-Access'** means that the public may inspect and obtain a copy of the information in a Court Record.

17. **'Open Access Data'** comprises Open Access Documents and Suo-motu Disclosures.

    (a) **Open Access Documents:** Information contained in the following Court Records is open-access and such Court Records are Open Access Documents:

        (i) a record of any judgment given and any direction given or order made in proceedings, including in connection with case management and court listing of proceedings, and including a record of a conviction in criminal proceedings
        (ii)a record of the dates on which proceedings are heard or to be heard and a record of the name of the judicial officer who heard or is officially listed to hear proceedings
        (iii)such other Court Records as may be prescribed by the Court

    (b) **Suo-moto Disclosures:** Information published by the courts pursuant to section 4(1)(b) of the Right to Information Act, 2005 and all other disclosures made on a suo-moto basis by the judiciary for public consumption are open-access.

18. **'Party'** shall include plaintiff, defendant, prosecutrix, accused, petitioner, respondent and appellant.

19. **'Personal data'** shall mean data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling, and shall include sensitive personal data.

20. **'Physical Access'** to Court Record is available at the appropriate Court Premises where such Court Record is maintained during normal working hours. Court Premises means and includes buildings and complexes under the authority of courts.

21. **'Policy' –** All references to Policy refer to the Judicial Information Management Policy in its entirety including Part I, Part II, Part III and Part IV, along with the annexures and schedules attached, unless the context otherwise requires.

22. **'Processing'**, in relation to personal data, shall mean an operation or set of operations performed on personal data, and may include operations such as collection, recording,

organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

23. **'Remote Access'** means the ability to electronically search, inspect, or copy information in a Court Record without the need to physically visit the court facility where the Court Record is maintained, and without needing the assistance of court personnel.

24. **'Restricted Access Data'** comprises Restricted Documents and Restricted Information.

(a)**Restricted Documents:** Any information contained in a Court Record that is not an Open Access Document is not open-access and such Court Record is a Restricted Document. Examples of Restricted Documents include transcription of proceedings, pleadings and written statements, affidavits, depositions etc.

(b)**Restricted Information:**Restricted Information comprises of the following information fields which may be contained both in Open Access Documents and Restricted Documents and is not open-access:

(i) financial information that provides identifying account numbers on specific assets, liabilities, accounts, credit cards, or tax identification numbers (PAN/TAN) of individuals or business entities and tax returns
(ii)AADHAAR number;
(iii)passport number;
(iv)personal telephone number and e-mail;
(v)date of birth (except year of birth);
(vi)names of minor children, witnesses, informants;
(vii) place of residence (except city/town/village and State)
(viii) psychological evaluations, Medical or mental health records, including examination, diagnosis, evaluation, or treatment records
(ix)description or analysis of a person's DNA or genetic material, or biometric identifiers
(x)other information that can be used to establish a person's identity and that is deemed by the court to constitute sensitive personal information

25. **'User Groups'** is aclassification based on which access under Part III of this Policy is determined in the manner provided below:

(a) **User Group 1: Judges and Judicial Officers**

'Chief Justice' means the Chief Justice of India and the Chief Justice of the High Courts , including the Acting Chief Justice, appointed under the Constitution of India.

'Other Judges of the Supreme Court of India and the High Courts' means a person appointed as a judge under Articles 124(2), 127, 217 or 224 of the Constitution of India.

'Judicial Officer' means a person appointed to judicial service as defined under Article 236(b) of the Constitution of India.

(b) **User Group 2: 'Court Staff'** means any person appointed to, employed by or authorised by the Court to exercise functions in a court registry or other court office such as to investigate or report on any matter of law or fact, or to make, authenticate, or keep any document, or to take charge or dispose of any property, or to execute any judicial process, or to administer any oath, or to interpret, or to preserve order in the Court. This includes a liquidator, receiver or commissioner who may be appointed by the Court.

(c) **User Group 3: Advocate of Record and Party of Record**

'Advocate of Record' means an advocate, who has entered an appearance, currently represents a party to the case, and who is listed as the advocate for that judicial proceeding in the case management system. It may include a firm or group of advocates acting on behalf of an agency or office, such as the Attorney General, Advocate General, Public Prosecutor etc.

'Party of Record' means a person who has been designated formally as a person engaged in a judicial proceeding. Party includes appellant(s), plaintiff(s), petitioner(s), complainant(s) and applicant(s) , defendant(s), respondents and judgment debtor(s).

(d) **User Group 4: 'Non-Party Interested Person'** means any non-party identified in a Court Record. This includes witnesses, experts, informants etc.

(e) **User Group 5: 'Law Enforcement Agency'** means a statutory body or an instrumentality of the Union or State government(s), authorized by law or by the government, to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law or breach of public order and safety and the execution of punishment and criminal penalties. [can add an inclusive list – police, CBI, NIA, ED etc]

(f) **User Group 6: 'Appropriate Government'** meansa governmental ministry, department, office or entity that interacts with courts on legal matters or cases.

(g) **User Group 7: 'Public'** means any person, natural or legal, who does not fall under User Groups 1 to 6.

Part II:

Policy on collection, processing, retention, storage and deletion

Clause 2: Enforcement authority

(1) The relevant authority responsible for carrying out the functions of the Court under this Policy shall be:

(a) for the Supreme Court, the [authority as designated by the Supreme Court]; and

(b) for each High Court and its respective subordinate courts, the [authority as designated by the High Court].

(2) The relevant authority of the Court shall undertake an annual review of the details within this Policy and its attached Schedule to update the retention and deletion timelines for personal data retained by the Courts and the eCourt project, if so required.

Clause 3: Processing for specific, clear and lawful purpose

No personal data shall be processed by the relevant authority except for any specific, clear and lawful purpose.

Clause 4: Collection limitation

(1) The personal data of the parties, witnesses, advocates or any other persons related to a case shall be collected only to the extent that it is necessary for the purposes of processing of such information.

(2) Where information is required for the purposes of judicial decision making, such information will include all information as can be required to be submitted to a judicial officer under any laws in force for the purposes of making a judicial determination on any point of law or fact in the case.

(3) Where personal data is collected for administrative purposes required for the discharge of judicial function:

(a) in case of a party to the case, it shall include:

1. information required to identify the party with reasonable certainty including name, age, gender; and
2. information required to expeditiously contact the party and to serve legal processes, including addresses, mobile numbers, email ID.

(b) in case of advocates, it shall include:

1. information required for identification including name, age, gender;
2. information required to expeditiously contact the advocate including addresses, mobile numbers, email ID; and
3. information regarding eligibility to file the case with the relevant judicial forum including bar council registration, being an advocate on record or any other similar qualification required to file the case.

(c) in case of witnesses, it shall include:

1. information required for identification including name, age, gender;

2. information required to expeditiously contact the witness and to serve legal processes, including addresses, mobile numbers, email ID; and
3. the party on whose behalf that witness is appearing and the case in which they are appearing.

(d) in case of a caveat application, it shall include:
1. information required for identification of the caveator and caveatee including name, age, gender; and
2. information required to expeditiously contact the caveator and caveatee and to serve legal processes, including addresses, mobile numbers, email ID;

(e) in case of any other application filed by an entity not covered in clause 4(3)(a) to (d) with the court either as part of a case that has been filed or otherwise, it shall include:
1. information required for identification of the applicant including name, age, gender; and
2. information required to expeditiously contact the applicant and any other entity relevant for the administration of the application and to serve legal processes, including addresses, mobile numbers, email ID;

Provided, that where a party or witness or caveator or caveatee is a minor or a person who has been assigned a legal guardian, corresponding details of the legal guardian of such minor or person shall also be collected.

(4) The relevant authority, may for reasons recorded in writing, ask for any other information for administrative purposes required for the discharge of judicial functions.

Clause 5: Purpose limitation

Every judicial officer processing personal data of the parties, witnesses, advocates or any other person related to a case shall process such personal data in a fair and reasonable matter for the purposes of:

(1) judicial decision making;

(2) for administrative purposes required for the discharge of judicial function; or

(3) public interest, including improvement of efficiency of courts, in a manner that does not infringe on the privacy of the concerned individuals.

Clause 6:Right to notice

(1) Every person whose personal data is being processed for judicial decision making, shall be given notice, at the time of collection as far as possible, of the scope of personal data being processed, and the purposes for which it is being processed.

Provided that where it is not possible to provide notice at the time of collection, it may be provided at any time as soon as reasonably possible.

(2) Every person whose data is being processed by the judiciary for purposes other than judicial decision making shall be given notice at the time of collection, of personal data being processed, and the purposes for which it is being processed.

Clause 7: Verification of information

(1) The relevant authority collecting details under clause 4(3) may require the concerned person to submit an officially valid document to authenticate the information provided by them, including:

(a) an Aadhaar card or proof of possession of an Aadhaar ID; or
(b) voter ID issued by the Election Commission of India; or
(c) passport; or
(d) driving license; or
(e) any other document deemed equivalent by the relevant authority, including such documents that are recognised as "officially valid documents" under the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

(2) Any person within the criteria described under clause 4(3) shall have the option to submit any officially valid document mentioned in sub-clause (a) as long as it authenticates the information provided by them.
Provided that in case the relevant authority is not satisfied with the authenticity of the submitted officially valid document, it may ask for alternative officially valid documents.

(3) The relevant authority shall use documents submitted for verification under this rule only for such purposes of verification, and shall not retain such document or information provided for in such document, after the verification is complete.

Clause 8: Information other than information fields provided under clause 4

(1) For any other data apart from data permitted to be collected under clause 4, the relevant authority shall seek the consent of the concerned person including:

(a) personal data collected from various online portals or applications owned and managed or e-services provisioned by the relevant authority, not required for the administrative purposes for discharge of judicial functions, including:

(i) user provided data such as username, password, personal data recorded within documents saved within the portal; and
(ii) any other data generated by user access and automatically collected by such portals and applications from such access and use.

(2) The consent of the concerned person shall be free from influence or coercion, informed, specific to the purpose of processing, clear and capable of being withdrawn.

(3) Every person whose personal data has been collected under this clause, shall be given notice, at the time of collection, of personal data being processed, and the purposes for which it is being processed.

Clause 9: Right to confirmation and access

(1) Any person whose personal data has been collected by the relevant judicial officer, for purposes other than judicial decision making, shall have the right to obtain in a clear, concise and easily comprehensible manner:

(a) confirmation whether their personal data is being processed or has been processed;

(b) the personal data that is being processed or has been processed or a summary thereof; and

(c) a brief summary of processing activities with respect to that personal data.

(2) Any person whose personal data has been processed, for administrative purposes required for the discharge of judicial function, shall have the right to access in one place the identities of those with whom his personal data has been shared by the relevant judicial officer along with the categories of personal data shared with them.

Clause 10: Right to correction

(1) Any person whose personal data is being or has been processed, for purposes other than judicial decision making, may having regard to the purposes for which personal data is processed, subject to such processes as provided by the officer in charge, shall have the right to apply for:
(a) correction of inaccurate or misleading personal data;
(b) completion of incomplete personal data; and
(c) updating of personal data that is out of date.

(2) The [Registrar/Designated Judge/ Designated Officer] may not allow such application for reasons to be recorded in writing.

(3) If the applicant is not satisfied with the reasons mentioned, they may require the [Registrar/Designated Judge/ Designated Officer] to indicate, alongside the relevant personal data, that the same has been disputed by them.

Clause 11: Storage of court records

(1) Subject to the terms of this Policy, all court records shall be stored and made accessible in a timely manner and shall be complete, machine-readable, non-discriminatory, and non-proprietary in nature.

(2) With regard to court records, each Court shall act in accordance with the procedure laid out under the Digital Preservation SOP, including but not limited to the procedures set out for digitization, verification, storage, search and retrieval, preservation, interoperability and adherence to ISO standards.

(3) Court records shall be digitized in accordance with the Digital Preservation SOP in each Court, with clear and trackable segregation of active court records and court records marked for preservation and archiving. The court records digitized by district courts shall be shared with the judicial digital repositories on a monthly basis.

(4) Court records shall be preserved in a manner that it should enable accessing parties to find, read, represent, render and interpret the information accurately, corresponding to the original record, along with all associated information necessary for proper comprehension in accordance with the access provisions under this Policy. Court records

shall be preserved in such a way that it will remain accessible, reliable, discoverable, authentic and usable for subsequent reference.

(5) The Supreme Court and each High Court must individually establish and maintain judicial digital repositories, for the purposes of storing court records, that are audited and certified as per the ISO 16363 standard, the ISO 27001 standard and other applicable ancillary standards prescribed under the Digital Preservation SOP.

(6) The judicial digital repositories for each High Court referred to in sub-clause (5) shall preserve court records processed by that High Court as well as all court records processed by the district courts under its administrative control. Each judicial digital repository shall comply with and use a standardized judicial digital preservation system designed to conform to the ISO 14721 'open archival information system' reference model.

Clause 12: Personal data retention for court records

(1) The references to personal data within each specific court record generated or stored by the Court, shall be retained, and thereafter deleted, in accordance with the timelines prescribed provided for the destruction of such court records within the applicable Court rules framed under the Destruction of Records Act, 1917;

Provided that no Court shall retain personal data beyond such time as may be required in the interests of transparency and public interest for court records generated or stored in the course of a judicial proceeding, which may be determined based on the nature of the case and the personal data being retained, or necessity involving the improvement of efficiency of court administration for those court records that have been generated or stored pertaining to the administration of the court or clerk of court office and not associated with any particular case;

Provided further that, in cases which statutorily require the protection of the identity of the accused or the victim, the personal data retained by the Court shall be redacted accordingly, to ensure compliance with the statutory protections.

(2) References to personal data processed and retained by the eCourts portal and its associated software applications shall be deleted in accordance with the timelines stated in Schedule I.

Part III:
Policy on Access to Court Records

Chapter I: Preliminary

Clause 13: Objects

The objects of this Part are:

(a)to promote consistency in the provision of access to Court Records across Courts in India

(b)to provide for open access to the public to certain Court Records to promote transparency and a greater understanding of the justice system

(c)to ensure that access to Court Records does not compromise the fair conduct of Court proceedings, the administration of justice, or the privacy or safety of participants in Court proceedings, by restricting access to certain Court Records

Clause 14: Application

This Part shall apply to all Court Records, regardless of the form of the Court Record, the method of recording the information in the Court Record or the method of storage of the information in the Court Record.

Chapter II: Entitlement to Access Court Record

Clause 15: Uniformity of Access

Every person will have the same access to Court Records under this [Part], except as provided in clauses 16 and 17.

Clause 16: Access to Open Access Information

Every person is entitled to access Open Access Information regardless of the User Group to which such person belongs, unless the Court otherwise orders in a particular case or category of cases.

Clause 17: Access to Restricted Access Information

1.Access to Restricted Access Information is determined by the User Group. Access is restricted to certain User Groups based on their role, the jurisdiction, case type, or for other reasons as may be determined by the Court.

2.Access to Restricted Access Information will be as per the Access Matrix provided in Schedule II of the Policy.

3.For User Group 1 and User Group 2, each Court must establish practices to ensure that Access to Restricted Access Information is limited to those individuals who require Access in performance of their official duties and specific employment responsibilities.

4.All applications under Clause 17 (2) must be made to [Registrar/ Designated Judge/ Designated Officer], unless specifically provided for otherwise in the Access Matrix.

5.The access granted under this clause is in addition to the access to Open Access Information.

6.All persons authorized under this Partto have greater access than the User Group 7 (Public) must protect records and information in strict accordance with applicable law including (i) all statutes, regulations, rules, judicial and administrative decisions, (ii) relevant industry guidelines, (iii) its own privacy policies, and (iv) contractual obligations, if any. Any entity provided with access to Restricted Access Information must establish policies and systems to ensure that such access is limited to those individuals who require access in performance of their official duties and immediately remove the individual at such time as the individual is no longer associated with that entity.

Clause 18: Request for Bulk Access/Distribution of Court Records

1.Requests for Bulk Access/ Distribution of Court Records should be made in the form prescribed in Schedule III to [Registrar/ Designated Judge/ Designated Officer].

2.Bulk Access/Distribution of Open Access Information

(a)Bulk Access/Distribution is automatically permitted for Open Access Information and should be made available via remote access to the extent that is technically and practically feasible.

(b)Applicants requesting Bulk Access/ Distribution of Open Access Information will not be required to provide any information beyond what is necessary to grant them access, such as their identity and contact information, and information necessary for them to pay fees. They shall not be required to provide any justifications for their request.

3.Bulk Access/Distribution of Restricted Access Information

(a)Bulk Access/Distribution to Restricted Access Information may be permitted on a request made by an applicant.

(b)The request shall:
(i) identify what information is sought,
(ii) describe the purpose for requesting the information
(iii) explain how such information will be securely protected

(c)Requests should only be allowed for purposes which are in public interest and facilitate the interests of justice in particular. These may include scholarly, journalistic, governmental, research, evaluation or statistical purposes where the identification of specific individuals is ancillary to the purpose of the inquiry.

(d)Requests may be rejected for any purposes that do not fulfill the criteria of Clauses 18(3)(b) and (c). In particular, Bulk Access/Distribution of Restricted Access Information must not be granted for:

(i) Surveillance, except as conducted by the competent authority, in fulfillment of its legal mandate, within the bounds of its enabling legislation and any other law in force;
(ii)Profiling, meaning any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
(iii)Unlawful discrimination

(e)If a request for Bulk Access/Distribution of Restricted Access Information is accepted, access to such information will be given under and governed by an agreement between the applicant and the Court, which may, in addition to other terms, include the following conditions:

(i)Access may be registered and logged. Upon request, such logs may be made available to members of the public, as determined by the Court
(ii) Applicant shall not access the data or disseminate any information obtained under the agreement except as necessary to fulfill the purposes for which access was granted.
(iii) The information may be regularly checked against the source of the court record for accuracy, especially if this information is to be published or redistributed
(iv)The information will not be used directly or indirectly to sell a product or service to an individual or the general public or for any other commercial purpose, except with the express permission of the court
(v)Any use of the information or data by the applicant should comply with all its contractual obligations as well as any other applicable law.

4.Where the volume of data requested under Clause 18(2) or Clause 18(3) exceeds a threshold prescribed by the Court, the applicant may be required to pay appropriate fees to meet the cost of providing the information. Fees may be levied at the discretion of the [Registrar/ Designated Judge/ Designated Officer] to whom the application is made for which a specific disclosure with respect to the purpose for which access is sought must be made. Generally, fees should be exempted when access is granted for research purposes, and fees should be levied when access to such data is used for any commercial purposes or to derive pecuniary gains.

Clause 19: Request for Access to Compiled Information

1.Requests for access to Compiled Information should be made in the form prescribed in Schedule III to [Registrar/ Designated Judge/ Designated Officer]

2.Access to Compiled Information - Open Access Information

Any person may request Compiled Information that consists solely of information that is Open Access Information. The Court may compile and provide the information if it determines, in its discretion, that providing the information meets criteria established by the Court, that the resources are available to compile the information and that it is an appropriate use of public resources.

3.Access to Compiled Information -Restricted Access Information

(a)Compiled information that comprises Restricted Access Information may be requested by any person only for the purposes which are in public interest and facilitate access to justice in particular. These may include scholarly, journalistic, governmental, research, evaluation or statistical purposes where the identification of specific individuals is ancillary to the purpose of the inquiry.

(b)The request shall:
(i) identify what information is sought
(ii)describe the purpose for requesting the information
(iii)explain how such information will be securely protected

(c)The Court may grant the request and compile the information if it determines that doing so meets criteria established by the court and is consistent with the purposes of this Part, the resources are available to compile the information, and that it is an appropriate use of public resources.

(d)If a request for access to Compiled Information is accepted under Clause 19(3), access to such information will be given under and governed by an agreement between the applicant and the Court , which may, in addition to other terms, include the following conditions:

(i)Access may be registered and logged. Upon request, such logs may be made available to members of the public, as determined by the Court.
(ii)Applicants shall not access the data or disseminate any information obtained under the agreement except as necessary to fulfill the purposes for which access was granted.
(iii)The information may be regularly checked against the source of the court record for accuracy, especially if this information is to be published or redistributed
(iv)The information will not be used directly or indirectly to sell a product or service to an individual or the general public or for any other commercial purpose, except with the express permission of the court
(v)Any use of the information or data by the applicant should comply with all its contractual obligations as well as any other applicable law.

4.Where the volume of data requested under Clause 19(2) or Clause 19(3) exceeds a threshold prescribed by the Court, the applicant may be required to pay appropriate fees to meet the cost of providing the information. Fees may be levied at the discretion of the officer [Registrar/ Designated Judge/ Designated Officer] to whom the application is made for which a specific disclosure with respect to the purpose for which access is sought must be made. Generally, fees should be exempted when access is granted for research purposes, and fees should be levied when access to such data is used for any commercial purposes or to derive pecuniary gains.

Clause 20: Request for Extended Access

1.Any person may make a request for access to a portion of the Court Record that is otherwise restricted pursuant to this Part. The request shall be made in the form prescribed in Schedule III.

2.In deciding whether or not access should be granted, and what specific terms and conditions should be imposed, including the possibility of registered access, the criteria specified in clause 22 shall be taken into consideration. The Court may require an undertaking or agreement to be signed prior to granting access under this clause.

Clause 21: Requests for limiting access

A request to prohibit access to information in a Court Record that a person is otherwise entitled to under this Part may be made by any Party, Interested Person, or on the Court's own motion. The Court must decide whether there are sufficient grounds to prohibit access according to applicable law and the criteria specified in Clause 10. In restricting access, the Court will use the least restrictive means that will achieve the objects of this Part enumerated in Clause 1 and the needs of the requestor.

Clause 22: Courts to consider certain factors while deciding applications under Clauses 17, 18, 19 , 20 and 21

A Court must take the following factors into account to the extent to which it considers them relevant while deciding applications made under Clauses 17, 18, 19, 20 and 21 in addition to any other factors that may be required under those clauses:

(a)the public interest in access to the information being provided
(b)the extent to which the principle of open justice will be adversely affected if access is not provided to the information
(c)the extent to which an individual's privacy or safety will be compromised by providing access to the information
(d)the extent to which providing access to the information will adversely affect the administration of justice
(e)the extent of the person's interest or involvement in the proceedings or other matter to which the information relates
(f)the reasons for which access is sought
(g)such other matters as the court considers relevant in the particular circumstances of the case

Clause 23: Method of Access

1. All User Groups are authorized for Remote Access to all Open Access Information.

2. Remote Access to Restricted Access Information is provided in certain situations as per clause 6 above.

3. Notwithstanding Clause 17 and Clause 23(2), there is no Remote Access for User Group 7 (Public) to Restricted Access Information in the following cases:

(a)Family Court proceedings, including proceedings for divorce, child and spousal support, child custody, adoption and domestic violence
(b)Juvenile Court proceedings
(c)Proceedings under Mental Health Act
(d)Proceedings to determine parentage
(e)Proceedings under Medical Termination of Pregnancy Act
(f)Cases concerning sexual offence, including POCSO
(g)Cases concerning gender-based violence against women
(h)Cases concerning offences relating to sovereignty and integrity of India and the security of the State
(i) any other case or type of case that the Court may determine

4. Security Requirement for Remote Access

(a)User Group (Judges and Judicial Officers), User Group 2 (Court Staff), User Group 3 (Attorneys of Record or Parties of Record), User Group 4 (Non-Party Interested Persons), User Group 5 (Law Enforcement Agencies), and User Group 6 (Governmental Partners) will require registration and verification of user role.

(b)User Group 7 (Public) will not be required to undergo any security clearance

5. If a Court Record to which remote access is permissible under this Part is not available or cannot be maintained in electronic form due to any reasons, physical exhibits of such records shall be made available for inspection during the office hours of the Court, in accordance with the appropriate access level. When remote access to Court Record is permissible under this Part and such remote access is available, even then the right to physically inspect the Court Record can be exercised and such right may not be restricted merely on account of remote access being available for such record.

Clause 24: Access under other laws

This Part is not intended to prevent or otherwise interfere with the giving of access to Court Record as permitted or required by or under any other Act or law that entitles a person to access Court Record.

Clause 25: Restrictions on access—court orders and other laws

1.There is no entitlement to access Court Record under this Part if providing that access would contravene:
(a)any order of a Court that prohibits or restricts the publication or disclosure of such information; or
(b)any provision made by or under any other statute or rule made thereunder that prohibits or restricts the publication or disclosure of such information

2.The Court may impose conditions on the way in which access to Court Record is to be provided under this Part or restrict the disclosure or use of Court Record to which access is provided under this Part.

3.The Court may refuse to provide access to Court Record that a person is otherwise entitled to under this Part and for reasons to be recorded in writing, if:

(a)providing access would require an unreasonable diversion of the Court's resources, or
(b)it is necessary to refuse access to ensure the safe custody and proper preservation of Court Records (but only if this cannot be ensured by the imposition of reasonable conditions on the provision of access).

Chapter III: Privacy Protections

Clause 26: Courts to publicize rules for accessing Courts Records and publish a privacy notice

1.The Court will make information available to litigants and the public that information in the Court Record about them is accessible to the public, including remotely and how to request to restrict the manner of access or to prohibit public access.

2.Each Court is to publish on its website, and by other appropriate means, general information that promotes awareness of the potential for information provided by a party to proceedings to be accessed by other persons pursuant to an entitlement under this Part and the Court's practices and procedures for preventing or limiting access to personal information, including a privacy notice. A draft privacy notice is provided in Schedule IV of this Policy.

3.Specific information which must be publicised by Courts must include the following

(a)Means of obtaining access to Court Record;
(b)When access is available;
(c)Procedure for requesting extended access or limiting access to certain Court Record;
(d)Procedure for requesting Bulk Access/Distribution and Compiled Information;
(e)Possible fees for obtaining access or copies;
(f)Consequences of failure to abide by this Part or any other conditions of access; and

(g)Complaint and grievance redressal procedure

Clause 27: Redaction, Anonymization of Personal identification information

1.For the purpose of facilitating access to Court Records, a Court must ensure to the maximum extent reasonably practicable that Court Records that contain Open Access Information do not contain personal identification information.

2.If documents defined to be Open Access Documents contain Restricted Information, such information must be suitably redacted/anonymised prior to publication, via means to be prescribed by the court, in a manner that best prevents re-identification/de-anonymisation.

Chapter IV: Security of Court Records

Clause 28: Security safeguards

A Court must take such adequate security safeguards as are reasonable in the circumstances to ensure that the court information contained in Court Record is protected against misuse and unauthorized access, use or disclosure.

Clause 29: Unauthorized disclosure and use of Court Record

1.A person who is provided with access to Court Record pursuant to an entitlement under this Part must not disclose or use the information for a purpose or in a manner that the person knows is contrary to any condition of access imposed by the Court or any other law.

2.A person must not disclose or use Court Record obtained in the exercise of the person's functions as a court officer or in the execution or administration of this Part except:
(a)with the consent of the person from whom the information was obtained, or
(b)in the exercise of those functions or in the execution or administration of this Part, or
(c)as otherwise authorized or required by law.
Provided, if a court officer discloses Court Record by providing access to the information and believes in good faith when providing access to the information that this Part permits or requires that access to be provided, the officer is deemed to have disclosed the information in the execution of this Part.

3.A person must not induce or attempt to induce another person to disclose or use Court Record in contravention of Clause 29(2).

Clause 30: Consequences of violation

Any person violating this Part is subject to partial or complete revocation of access for a duration to be determined by the Court.

Part IV:

Policy on Complaints Handling

Clause 33: Committee for handling complaints regarding the Policy

a) The Committee shall consist of a chairperson and two members, chosen from among the Judges of the High Court.
b) The chairperson and the Committee members shall be appointed by the Hon'ble Chief Justice of the High Court
c) The term of the members of the Committee, including the chairperson, shall be subject to the discretion of the Hon'ble Chief Justice of the High Court.
Provided that the chairperson shall have a tenure of at least one year.
d) The Chief Justice shall endeavour to fill up any vacancy in the office of a member of the Committee or the chairperson within a period of 30 days from the date of the vacancy arising.
e) The Committee shall meet when convened by the chairperson. However, the Committee shall endeavour to hold a sitting once every 30 days. The quorum for such meetings shall be achieved if the chairperson and one member of the Committee are present.
f) The Committee may invite technical members, and members from the Bar to assist the Committee in handling complaints related to the Policy.
Provided that the technical members and members from the Bar shall not exercise any decision making power, and maintain confidentiality regarding the proceedings of the Committee.
Provided further that the technical member must have experience in the field of information technology.

Clause 34: Functions of the Compliance Officer

a) To promote awareness of data protection and the Policy amongst courts and tribunals within the territory of the High Court.
b) Arrange periodic training for judges and court staff of the High Court and the District Judiciary within its jurisdiction to ensure compliance with the Policy.
c) Provide a Frequently Asked Questions (FAQ), tutorial video, or any other material on the website of the High Court, which will enable the public to understand the grievance redressal mechanism provided in Clause 6 and Clause 7.
d) Auditing practices of courts periodically to ensure compliance with the provisions of the Policy.
e) Investigating non-compliance with the Policy.
f) Addressing a representation to the Grievance Redressal Officer if it finds non-compliance with the Policy.
g) Appoint nodal officers in every District Court within the jurisdiction of the High Court. The nodal officers shall assist data principals in addressing representations to the Grievance Redressal Officer.

Clause 35: Functions of the Grievance Redressal Officer

a) To respond to representations against non-compliance of the Policy including those representations by the Compliance Officer.

b) To refer to the Committee any representation which seeks erasure or redaction of personal data or challenges the processing of personal data.
c) To prepare and submit to the Chief Justice on a quarterly basis a consolidated report which provides information regarding the total number of representations received by the Grievance Redressal Officer and the action taken thereon.

Clause 36: Reliefs a Data Principal may seek

In accordance with rights recognised by Part II of this Policy, the kind of reliefs a Data Principal may seek under these rules may include:

a) Seeking confirmation that their Personal Data has been processed;
b) Accessing a copy of their Personal Data;
*Provided that the High Court of *Judicature* may charge a reasonable fee to provide a copy in case the Data Principal's Personal Data is found to be excessive.*
c) Asking for Personal Data to be corrected, erased, redacted, or for restrictions to be placed on how it is processed;
d) Challenging or objecting to Personal Data being processed in violation of this Policy;
e) Seeking transfer of Personal Data to a third party;
f) Seeking blocking of non-judicial data processing;
g) Seeking grievance redressal for violation of any part of this Policy; and
h) Seeking similar reliefs on behalf of a Data Principal subject to establishing *bona fides* before the Committee or before the Grievance Redressal Officer, as the case may be.

Clause 37: Procedure to institute representations regarding non-compliance with the Policy

a) A Data Principal aggrieved by non-compliance with the Policy or a Compliance Officer who has found non-compliance with the Policy may address a representation by email or by post to the Grievance Redressal Officer. The Data Principal shall raise any such representation by filing the form prescribed in Schedule V and providing reasons for their request. Such a representation shall be made in one of the official languages of the High Court of *Judicature*
b) The Grievance Redressal Officer shall acknowledge the receipt of the representation within a period of 7 days.
c) The Grievance Redressal Officer shall refer to the Committee any representation seeking withdrawal of consent to process data or asking for personal data to be erased or redacted or challenging the processing of personal data.Any such reference must be made within 7 days from the date of acknowledging the receipt of the representation under Clause 37(b).
d) In case of any representation which is not covered within Clause 37(c), the Grievance Redressal Officer shall, by a reasoned order, grant or refuse to grant, in whole or in part, the relief sought by the Data Principal or the Compliance Officer within a period of 60 days.
e) All decisions of the Grievance Redressal Officer shall be subject to the approval of the Chief Justice and such approvals must be sought within the timeline mentioned in Clause 37(d).
f) The decision of the Grievance Redressal Officer must be made available to the Data Principals once it is approved by the Chief Justice.

Clause 38: Procedure to seek review of the decision the Grievance Redressal Officer

a) A review application may be made by the Compliance Officer or the Data Principal to the Committee regarding the decision taken by the Grievance Redressal Officer within a period of 14 days from the date of the decision. A Data Principal may also prefer an application to the Committee in case the Grievance Redressal Officer does not decide their application within the prescribed time period. Provided such an application is preferred within a period of 14 days from the date on which the date on which Grievance Redressal Officer should have decided the Data Principal's application.
b) The review application shall be made in one of the official languages of the High Court of *Judicature* and by filling the form prescribed in Schedule VI.
c) The Committee shall provide an opportunity of hearing to the Data Principal.
d) Upon review, the Committee may, by a reasoned order, annul, vary or uphold the decision of the Grievance Redressal Officer. In the event, the Committee is seized of the reference under Rule 37(c), the Committee may, by a reasoned order, grant or refuse to grant, in whole or in part, the relief sought by the Data Principal.
e) The Committee shall endeavour to decide upon the review or the reference within a period of 90 days from the date of the institution of the review or the reference, as the case may be.
f) All decisions of the Committee shall be subject to the approval of the Chief Justice and such an approval ought to be sought within the timeline mentioned in Clause 38(f).
g) The decision of the Committee must be made available to the Data Principal once it is approved by the Chief Justice

Part V:

Miscellaneous

Clause 39: Supreme Court and High Courts to make rules pursuant to this Policy

The Supreme Court of India and the High Courts shall make rules, for or with respect to any matter that by this Policy is required or permitted to be prescribed by rules or that is necessary or convenient to be prescribed by rules for carrying out or giving effect to this Policy in all courts under its jurisdiction.

Clause 40: Immunity from liability in respect of disclosure of Court Record

1.The Court, any judge or judicial officer and any Court Staff responsible for receiving, disseminating, handling, managing, or processing Court Records will have immunity in respect of any inaccuracies or outcomes of secondary use of Court Records obtained by applicants for Bulk Access/ Distribution or Extended Access.

2.Such persons must not disclose or use Court Record obtained in the exercise of the person's official functions or in the execution or administration of this Part except:
(a)with the consent of the person from whom the information was obtained; or
(b)in the exercise of those functions or in the execution or administration of this Part; or
(c)as otherwise authorised or required by law

3. No judge, judicial officer, Court Staff, or any person acting under their direction shall be personally liable under this Policy for any matter or thing done by them, if such matter or thing was done in good faith for the purposes of executing this Policy.

SCHEDULE I

[Referred to in Clause 12 of Part II]

References to personal data within the following records shall be retained for, and deleted subsequent to, the following timelines:

Records containing personal data	**Personal data potentially available**	**Timeline for Retention**
Automatically collected data from E-Courts portal and associated applications	Portal- the user's server address; the name of the top-level domain from which users access the Internet (for example, .gov, .com, .in, etc.); the type of browser used; the date and time users access the site; the pages users have accessed. Application- mobile device type, mobile device's unique device ID, the IP address of the mobile device, mobile operating system, the type of mobile Internet browsers used by the	2 months

Records containing personal data	**Personal data potentially available**	**Timeline for Retention**
	user, and information about the way the user uses the application.	
User provided information within the e-Court portal or app collected for e-filing purposes	Username, password, advocate personal information recorded and saved within the portal or associated applications	Data retention shall be based on the purpose of deactivation of account, and the personal data retained shall be deleted: (a) 6 years after the deactivation of account on account of death of user; and (b) 6 years after deactivation of account on account of inactive or suspended Bar Council license/ certificate of practice. In this period, the user account may be reactivated through revocation of suspension or renewal of Bar Council license/ certificate of practice.

Records containing personal data	**Personal data potentially available**	**Timeline for Retention**
Information collected by court websites/eCourt portal for authentication of User Groups 1-6	[Varying data points to authenticate various User Groups. For example Judges in User Group 1 may be required to share details that verifies their role for allowing them access to the matter, litigating advocates in User Group 2 may required to show Bar Council license, and *vakalatnama* etc to show that they are retained for that matter etc.]	[-]

SCHEDULE II

Access Matrix referred to in Clause 17(2) of Part III

User Group	Access to Restricted Access Information			
	Restricted Documents		Restricted Information	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
User Group 1: Judges and Judicial Officers				
1. Chief Justices	Yes, for all data in their respective jurisdiction	Both	Yes, for all data in their respective jurisdiction	Both
2. Other Judges of Supreme Court of India and High Courts				
(a) When performing judicial	Yes, for their respective jurisdictions	Both	Yes, for their respective jurisdictions	Both

User Group	Access to Restricted Access Information			
	Restricted Documents		**Restricted Information**	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
function (b) When performing administrative function	(i) Yes, only for jurisdictions under their supervision. (ii) Generally, no for all other jurisdictions not under his supervision; In such cases, access may be granted on showing that such Restricted Document is necessary for the effective performance of their duties. Applications in this regard may be made to [Chief Justice.]	Both	(i) Yes, only for jurisdictions under their supervision. (ii) Generally, no for all other jurisdictions not under his supervision; In such cases, access may be granted on showing that such Restricted Information is necessary for the effective performance of their duties. Applications in this regard may be made to [Chief Justice.]	Both

User Group	Access to Restricted Access Information			
	Restricted Documents		**Restricted Information**	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
3. Judicial Officers				
(a) When performing judicial function	Yes, for their respective jurisdictions	Both	Yes, for their respective jurisdictions	Both
(b) When performing administrative function	(i) Yes, only for jurisdictions under their supervision. (ii) Generally, no for all other jurisdictions not under his supervision; In such cases, access may be granted on showing that such Restricted Document is necessary for the performance of their duties. Applications in this regard may be made to [Chief Justice.]	Both	(i) Yes, only for jurisdictions under their supervision. (ii) Generally, no for all other jurisdictions not under his supervision; In such cases, access may be granted on showing that such Restricted Information is necessary for the performance of their duties. Applications in this regard may be made to [Chief Justice.]	Both

User Group	Access to Restricted Access Information			
	Restricted Documents		**Restricted Information**	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
User Group 2: Court Staff	Yes, limited to jurisdiction in which they are employed and access to such Restricted Documents is necessary for the performance of their duties	Both	Yes, limited to jurisdiction in which they are employed and access to such Restricted Information is necessary for the performance of their duties	Both
User Group 3: Advocate of Record and Party of Record	Yes, only for the particular case; However, access will be changed to User Group 7 (Public) when the advocate's appearance is terminated in the particular case.	Both	Yes, only for the particular case; However, access will be changed to User Group 7 (Public) when the advocate's appearance is terminated in the particular case.	Both
User Group 4: Non-Party Interested Persons	(i) Yes, only for the Restricted Documents originating from such persons; (ii) For all other Restricted	Both Both	(i) Yes, only for the Restricted Information originating from such persons; (ii) For all other Restricted	Both Both

User Group	Access to Restricted Access Information			
	Restricted Documents		**Restricted Information**	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
	Documents not originating from such persons, must show good cause.		Information not originating from such persons, must show good cause.	
User Group 5: **Law Enforcement Agency**	(i) Yes, only for the Restricted Documents originating from such law enforcement authority; (ii) For all other Restricted Documents not originating from the law enforcement authorities, must show cause as to how access to such information is necessary for the maintenance of law and order;	Both Both	(i) Yes, only for the Restricted Information originating from such law enforcement authority; (ii) For all other Restricted Information not originating from the law enforcement authorities, must show cause as to how access to such information is necessary for the maintenance of law and order;	Both Both

User Group	Access to Restricted Access Information			
	Restricted Documents		**Restricted Information**	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
User Group 6: Appropriate Government	(i) Yes, only for the Restricted Documents originating from such authorities; (ii) For all other Restricted Access Information not originating from such authorities, must show cause as to how access to such information is necessary for the performance of their official duties.	Both Both	(i) Yes, only for the Restricted Information originating from such authorities; (ii) For all other Restricted Information not originating from such authorities, must show cause as to how access to such information is necessary for the performance of their official duties	Both Both
User Group 7: Public	Generally, No; Access may be granted on showing sufficient cause.	If Access is permitted, generally Physical/ Courtroom access only; Remote access may be permitted by the court in exceptional cases on showing sufficient cause	Generally, No; Access may be granted in exceptional cases on showing sufficient cause, and for reasons to be recorded in writing.	If Access is permitted, generally Physical/ Courtroom access only; Remote access may be permitted by the court in exceptional cases on showing sufficient cause and for

User Group	Access to Restricted Access Information			
	Restricted Documents		Restricted Information	
	Whether Access Permitted?	**Method of Access: Remote Access or Physical Access**	**Whether Access Permitted?**	**Method of Access: Remote Access or Physical Access**
		and for reasons to be recorded in writing		reasons to be recorded in writing

SCHEDULE III

Application for Requesting
Bulk Access to Court Records (referred to in Clause 18),
Access to Compiled Information (referred to in Clause 19), and
Extended Access (referred to in Clause 20)

[Insert Court Address, Contact information and Logo Here]

(I) The Applicant

1. Name(s) of the applicant/organization(s) and email address(es) that should be used to send the Court Record. If more than one organization is involved in the application, explain how they are affiliated?

   Note: If you wish to receive the information sought by mail, please provide us with your complete mailing address.

2. Provide information about the specific group(s) within your organization (e.g. corporate services, research team, etc.) that will be using such information, including the purpose for which it will be used.

(II) The Purpose

3. Describe the purpose for which the Court Record will be collected, used, and/or distributed and why such information is necessary. Also, identify the legislative authority, if any, for the collection, use, and distribution of the Court Record and whether the information is being collected for commercial use by the applicant.

4. The purpose of providing access to Court Record is to better facilitate the administration of justice and to improve access to Court Record where the public interest is served. Explain how the applicant's use and/or proposed distribution of the information contained in Court Records sought supports the primary purposes mentioned above.

(III) The Information

5. Identify the Court Record that you wish to collect, use, and/or distribute. Be as specific as possible by identifying the court level, the data elements, the documents, and the timeframes. If requesting access to Court Record from more than one level of court, list the information from each court separately.

6. Identify whether or not this court information is available from any other source(s).

7. Describe how the information will be used.

(IV) Form of Access

8. Describe the type of access requested (e.g. paper records or electronic records).

(V) User Access

9. In the following table, identify who will have access to the court record information.

User name	**Title**	**Contact Information (email address, telephone and/or mailing address)**

10. Describe why these users require access.

11. Have these users been screened for security purposes? If so, identify the security clearance level of each user who has been screened and briefly describe the method of screening.

12. Are all the users under the direct supervision of the applicant (e.g. are any users located at a different facility or under the supervision of a different organization)?

13. Which user will have the primary responsibility for the care and control of the Court Record / information and what is his/her relationship to each of the other users (e.g., research supervisor responsible for direct supervision of each user)?

(VI) Copying, Storing and Distributing Information

14. Will copies be made of the Court Record/ information and, if so, why?

15. Describe how copies of the Court Record/ information will be securely stored by the applicant.

16. Describe how the Court Record/ information will be shared, distributed or published and to whom? If applicable, it is necessary to specify the legal authority of the applicant for the sharing and distribution of court record information. Explain why it is necessary to include personal identifying information in suchsharing, distribution and/or publication. Alternatively, you must undertake to obliterate or remove such court record information before sharing, distributing and/or publishing.

17. What is your plan for the retention and disposal of the Court Record/ information after its use?

(VII) Security and Privacy of Information

18. What are the security arrangements for the protection of the Court Record/ information? For example, will it be stored on stand-alone computers controlled by the applicant, will information be stored "in the cloud" or accessed remotely, will information be password protected, and what security measures including

authentication measures are used by the applicant?

19. Having regard to legislative security and privacy requirements, what policies and procedures of the applicant are designed to meet the legislative requirements? For example, policies and procedures for correcting inaccurate information, and for meeting the requirements of protection of personal information legislation.

(VIII) Undertaking Statement

20. By checking this box , the applicant undertakes the following:

(a) Applicant shall comply with all current and, as subsequently amended, laws, court orders, administrative rules and policies governing, regulating, and/or relating to Court Records.

(b) Applicant will not re-broadcast or publish the information received outside the parameters identified in this application. Specifically, applicant shall not:

i. reproduce, resell or otherwise distribute, directly or indirectly;

ii. use, directly or indirectly, for the purpose of sale of a product or service to an individual or the general public; or

iii. copy or duplicate, other than as stated for scholarly , journalistic, political, governmental, research, evaluation or statistical purposes the Court Records/information

(c) Applicant will notify its employees, agents, clients, customers, and other third party recipients of the Court Record/information of the limitations on use of, and requirements for verification of, the Court Record/information obtained

(d) Upon notice from the Court, the applicant agrees to remove from its files within 24 hours any Court Record/information that has been amended, corrected, sealed, or otherwise restricted and notify its subscribers to do the same. The notice from the Court shall identify the cases that are to be corrected, removed, or otherwise restricted.

(e) Applicant shall remove all personal information that is inadvertently included in the Court Records/information provided to them and take other appropriate action to ensure that such personal information is not disclosed to others. Upon notice, the Applicant shall comply with future orders to scrub data if they should arise. [Not applicable when access to personal information has been requested by the applicant and such request has been accepted]

(f) Applicant understands and acknowledges that all rights, title and interests, including all intellectual property rights, in and to the Court Records or any other information provided to the applicant shall remain with the Court.

(g) Applicant shall not make bulk distribution of the Court Records or reconfigure the Court Records for subsequent bulk distributions.

(h) Applicant agrees that the Court may audit applicant's compliance with the terms and conditions on which access to Court Record/information has been granted and that the applicant will cooperate fully with any law enforcement investigation concerning the use of the Court Record/information by the applicant or its employees, agents, clients, customers, and other third party recipients of the Court Records/information provided pursuant to this application.

(i) Applicant acknowledges and accepts that the Court Records/information are provided "as is" and may include errors or omissions and, therefore the Applicant agrees, that Court and its officers shall not be responsible or liable for any demand or claim, regardless of the form of action, for any damages resulting from the use of such Court Records/information by the Applicant or its employees, agents, clients, customers, and other third party recipients of the Court Records/information.

(j) Applicant shall defend, indemnify, and hold harmless the Court and its officers against all claims, demands, suits, actions, judgments, damages, loss or risk of loss (including expenses, costs, and

reasonable attorney fees) of any and every kind and by whomever and whenever alleged or asserted arising out of or related to any use, distribution or transfer made of the Court Records/information by the Applicant and its employees, agents, clients, customers, and other third party recipients of the Court Records/information provided pursuant to this application.

(k) Applicant may not, without the express written permission of the Court, transfer or assign any right or benefit accruing to the Applicant or any claim arising pursuant to the acceptance of the request made in this application.

(l) The Applicant shall forthwith inform the Court in case there is a change in the purpose for which they sought bulk access to court records and shall submit the application afresh.

(m) The Applicant shall forthwith inform the Court if there is a security breach in their computer systems which store the Court Records and shall take such steps as may be prescribed by the Court to ensure the protection of the data.

(n) The Applicant shall not act in contravention of this undertaking and if they do so, the Court reserves the right to restrict access to Court Records without any prior notice.

(IX) How to Submit your Application

21. Once your application is complete, please send it as an email attachment to: (_____) OR If you prefer to send your application form by mail, please send it to the following mailing address: (_____

(X) Summary (for office use only)

22. Access approved ( ) OR Access denied ( )

23. Name and title of assessor:

Name(s)	Title(s)	Contact Information

24. General Comments (if applicable):

SCHEDULE IV

Draft Privacy Notice referred to in Clause 26(2) of Part III

The [specific court] respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when we are performing our necessary functions or when you contact us. This includes online channels.

If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact us using the details set out below.

Contact Person:[Designated officer]

Phone:[-]

Email:[-]

1) What personal data do the courts collect from you?

Your personal data refers to any information about you that can be used to identify you. It includes information about you such as your name and contact details. Other fields of personal data include information about your gender, sex, religious beliefs and caste. The Court can collect any such personal data, in accordance with the Judicial Data Management Policy ("**the Policy**"), that it deems necessary for the discharge of its judicial function.

The nature of your personal data collected will significantly depend on the reason for which you are coming before the Court. For example, at the most preliminary level of registration of the case, the registry of the relevant court will require name and contact information of the parties and the counsels. Further processing of personal information will be dependent on a case to case basis. For example, in case of a bail application, the court will require your name and contact information, along with all other information that the court deems necessary to decide whether or not your bail application is to be granted. The court may further require personal data about you in an ongoing manner that is necessary for the satisfaction of the court that the bail conditions are being adhered to.

2) For what purposes can your personal data be processed by courts?

The Court collects your personal data for the purpose of discharge of judicial functions. Judicial functions primarily include two kinds of functions. These are, first, judicial decision making, and second, administrative functions of the Court. Judicial functions of the court mean its function of deciding an application, case or other judicial matter before the court. Calling for personal information for discharge of judicial functions would mean personal information that is required to make a judicial determination in an ongoing matter. For example, in matters of sexual harassment, the court may require the parties to produce records of personal communications between them. The court is the sole authority for determination of the personal information required to discharge judicial decision making function. The administrative functions of court are required to discharge and aid judicial decision making and maintain its administration. For example, while registering your case, your identity and contact details will be required by the respective registrar.

3) What is the legal basis for processing your personal data by courts?

This courts derives the powers to discharge these functions from [constitution][crpc][state acts][high court rules]

3) How is your personal data collected?

The courts can receive personal data about you from a number of sources including:

(a) provided by you (in whichever capacity you appear before the court and legal obligations attendant thereto);
(b) From parties to proceedings (a plaintiff, a defendant), or their legal advisors; a witness giving evidence before the court;
(c) Law enforcement agencies;
(d) A person who is not a party to proceedings, but who is required to provide discovery (a pre-trial procedure); and
(e) Any other publicly available information (for example from other reported cases).

4) What do we mean by processing?

Processing with respect to your personal data means the entire range of actions taken by us. This includes operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

5) What happens if you fail to provide your personal data?

You are under a legal obligation to provide information to the court. This legal obligation stems from various laws which provide judicial officers the power to call for information. The consequences for failure to provide information will be determined by the court in accordance with the law under which you are obligated to provide that information. This policy itself does not impose any legal consequences for non furnishing of the requisite information.

6) How long is your personal data retained for?

The Courts retain and subsequently delete your personal data recorded within the court records in accordance with clause 12 of the Policy. In the absence of any retention period under law or under Part II of the Policy, the Court shall not retain your personal data any longer than necessary with regard to public interest, transparency or for the efficient administration of courts. Furthermore, references to personal data within court records shall compulsorily be deleted in accordance with the applicable court rules pertaining to destruction of court records.

7) Disclosures/Sharing of your personal data

Court and tribunal proceedings are, except in exceptional circumstances or where required by law, such as rules of court or a court or tribunal order or statute, required to be held in public. This is an aspect of the constitutional right to open justice. There is generally therefore no expectation of privacy in personal data which is processed by the judiciary exercising judicial functions.

Personal data that is contained in court records can be made available to people and organisations that are entitled or permitted to access court records in accordance with Part III of the Policy and under other applicable law. For example, your personal data may be shared by the judiciary with, but not limited to,

- A party to the proceedings concerned, or that party's legal representative;
- Members of the press or broadcast media that have sufficient proof of their status for the purpose of facilitating the fair and accurate reporting of a hearing in the proceedings;

- Members of the public - In accordance with the requirements of the Constitution, proceedings are generally held in public save in such special and limited cases as may be prescribed by law. This means that information that is disclosed in a court will be heard by those in attendance;
- Other third parties for whose involvement provision is made by statutes, court rules, or practice like law enforcement bodies, government departments and agencies etc

The Courts also require the assistance of third-parties, for example, IT service providers, in order to operate. These third parties may be given access to personal data that is processed by the courts in the provision of their services. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions. We require all third parties to respect the security of your personal data and to treat it in accordance with the law.
Personal data may also be shared with other courts and tribunals in other countries where this is necessary further to the administration of justice or to comply with, or to fulfil, legal obligations.

8) Publication of your personal data

Personal data processed by the judiciary exercising judicial functions may be published in court or tribunal orders or judgments or in a list or schedule of proceedings or hearings, in accordance with the constitutional requirement that proceedings be generally held in public.
Personal data of certain individuals may also be published when required under law, for example, under the Right to Information Act, 2005. This is necessary in the public interest of the administration of justice. It is necessary to enable individuals to understand their rights and obligations, which is an aspect of the rule of law. Publication of judgments is also a requirement of the constitutional principle of open justice and is a necessary means to support the rule of law. As such it is in the public interest.

A Court or tribunal may, where it is strictly necessary in the interests of the administration of justice, place restrictions on personal data, such as an individual's name, which is placed in a judgment. It may also hold legal proceedings in private and place restrictions on access to court records in accordance with the Part III of the Policy. Such decisions are judicial decisions and can only be taken within legal proceedings. Individuals wishing to raise such matters should seek legal advice.

9) International transfers of your personal data

The Courts may in certain circumstances where this is permitted by law or by the express permission of the Court (for example in matters of judicial co-operation and criminal justice mutual assistance and whether the transcription of digital audio records of proceedings is carried out in a third country) transfer or have transferred on their behalf personal data outside India.

10)Data Security

Courts have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, accessed, altered or disclosed in an unauthorised way. In addition, Courts limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on the Court's instructions and they are subject to a duty of confidentiality.

Courts have also put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach.

11) What rights do you have with respect to personal data we hold about you

- Request access to your personal data
- Request correction of the personal data that we hold about you
- Request erasure of your personal data
- Request restriction of processing of your personal data
- Object to processing of your personal data in violation of this Policy
- Request the transfer of your personal data to you or to a third party
- Any other rights given under the grievance redressal policy

12) How do you exercise your rights?/How to submit a complaint?

Address a representation: If you are aggrieved by non-compliance with the Policy, may address a representation to the Grievance Redressal Officer by sending an email at _____ (email of Greivance Redressal Officer) or posting a letter at _____ (address of Greivance Redressal Officer). You must make the representation by filing a form provided in Schedule V of the Policy.

Responsibility of Grievance Redressal Officer: The Grievance Redressal Officer must acknowledge the receipt of the representation within a period of 7 days and shall refer to the Committee any representation seeking withdrawal of consent to process data or asking for personal data to be erased or redacted or challenging the processing of personal data within 7 days from the date of acknowledging the receipt of the representation. The Committee, in turn, has the decision to grant or refuse to grant the relief sought by you.

In case of representations that are not referred to the Committee, the Grievance Redressal Officer shall respond to you within a period of 30 days. Upon expiry of that period, failure to reply is deemed to constitute an implied decision acceptance of your application.

Appeal: You may approach the Committee regarding decisions taken by the Grievance Redressal Officer by sending an email at _____ (email of the Committee) or posting a letter at _____ (address of Committee). You must appeal within a period of 14 days of the decision of the Grievance Redressal, and the Committee may annul, vary or uphold the decision of the Grievance Redressal Officer.

13) No fee usually required

You will not have to pay a fee to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

14) What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data or to exercise any of your other rights. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

15) Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

16) Changes to the privacy notice and your duty to inform us of changes

The Court may amend the privacy notice. The version date of this privacy notice indicates the date of the most recent amendment. The version date of the current statement is ().

It is important that the personal data that the Court holds about you is accurate and current. Please keep the Court informed if your personal data changes during your relationship with it.

17) Third party links

This website may include links to third party websites. Clicking on those links may allow third parties to collect or share data about you. We do not control these third party websites and are not responsible for their privacy statements.

18) Site Data

If you are a user with general public and anonymous access (User Group 7), the Court website does not store or capture personal information but merely logs the [user's IP address, users server's address, the name of the top-level domain from which users access the Internet (for example, .gov, .com, .in, etc.), the type of browser users used, the date and time users access the site, and the pages users have accessed or their browsing activities are not identified by the Court website, except when a law enforcement agency may exercise a warrant to inspect the service provider's logs that is automatically recognised by the web server]. Additional information may be required for the purposes of authenticating access to User Groups 1 to 6.

[*Please note that the data fields for information collected may change based on the purposes and functions of specific sub-projects and websites within the eCourts project.*]

The system may record your email address and other information if volunteered to us by you. This shall be treated as proprietary and confidential. It may be used for internal review and to notify you about updates to the Court's website.

19) Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. You will receive communications from us if you have requested information from us or if you provided us with your details when you entered a competition.

20) Opting out

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time.

SCHEDULE V

[Referred to in Clause 37(a)]

Representation to the Grievance Redressal Officer

1. Applicant Details:
    a. Name:
    b. Address:
    c. Phone number:
2. Diary Number / Filing Number (if any):
3. Cause Title:
4. Whether the reliefs sought, relate to the Applicant? Y/N
5. If the answer to 4 is no, please state the Applicant's relationship to the person and why this application is being preferred. Provided a signed confirmation that the Applicant has the permission or the authority to act on their behalf.
6. Whether the Representation needs to be referred to the Committee under Clause 37(c)? Y/N
7. Grievance with non-compliance of the Policy:
8. Reasons:

I have read and understood the Judicial Information Management Policy. I undertake to remain bound by the same to the extent applicable to me.

Signature of the Applicant

(this application may be e-signed)

Date:

SCHEDULE VI

[Referred to in Clause 38(b)]

Review Application to the Committee

1. Applicant's Details:
    a. Name:
    b. Address:
    c. Phone number:
2. Diary Number / Filing Number (if any):
3. Cause Title:
4. Reasons for complaining against the decision of the Grievance Redressal Officer:

I have read and understood the Judicial Information Management Policy. I undertake to remain bound by the same to the extent applicable to me.

I also submit that I have attached a true copy of the representation addressed to the Grievance Redressal Officer and the decision of the Grievance Redressal Officer.

Signature of the Applicant/Authorised Representative

(this application may be e-signed)

Date:

SECTION 5: PRACTICE NOTES FOR COURT STAFF AND JUDGES
[In progress - to be compiled based on feedback and pilot projects]

SECTION 6: FAQs FOR CITIZENS AND LITIGANTS [In progress]

SECTION 7: PILOT PROJECTS

It is suggested that pilot projects be initiated to:

- get a deeper understanding of processes, response of stakeholders involved, and the technological capacity/changes to implement the policy; and
- receive feedback on changes required to be made to the policy

The first pilot project will:

1. Ensure depositions for any of the case types are not made available publicly.
2. Create a separate case type of Prohibition of Child Marriage Act, 2006 and disable public availability of its data.
3. Create a separate case type for Termination of Medical Pregnancy Act, 1971 and disable public availability of its data.
4. Review the list of case types for which masking/redaction is currently enabled in Case Iinformation System (Juvenile Justice, POCSO, Domestic Violence, etc), study its functioning, and changes required to it.
5. Review data collection, processing, and storage practices for the above types of cases; compare with recommendations of the Policy.

The locations for the pilot could tentatively be one district and the High Courts selected for geographical distribution.