
Specialist Certification in Digital Preservation

Copyright and Intellectual Property Rights

Copyright and Intellectual Property Rights

Copyright and intellectual property rights are fundamental concepts in the field of digital preservation. They play a crucial role in determining how digital content can be used, shared, and preserved. Understanding these concepts is essential for digital preservation specialists to ensure that they comply with legal requirements and best practices in managing digital collections.

Copyright is a legal right that grants the creator of an original work exclusive rights to its use and distribution. This includes the right to reproduce, distribute, display, and perform the work. Copyright protection is automatic and begins as soon as a work is created and fixed in a tangible form, such as a digital file. In the context of digital preservation, copyright law applies to a wide range of digital content, including text, images, audio, video, and software.

Intellectual property rights encompass a broader set of legal rights that protect various types of intellectual creations, including patents, trademarks, and trade secrets. In the context of digital preservation, intellectual property rights are primarily concerned with copyright law, which governs the use and distribution of digital content. Digital preservation specialists must be aware of these rights to ensure that they comply with legal requirements when managing digital collections.

Related Terms: Fair Use, Public Domain, Creative Commons, Digital Rights Management (DRM)

Explanation: Copyright and intellectual property rights are essential considerations in digital preservation. Digital preservation specialists must be aware of these concepts to ensure that they comply with legal requirements when managing digital collections. By understanding copyright law and intellectual property rights, specialists can navigate the complex legal landscape surrounding digital content and make informed decisions about how to preserve and provide access to digital materials.

Example: A digital preservation specialist is tasked with archiving a collection of photographs from a local historical society. Before digitizing and making the photographs available online, the specialist must determine whether the photographs are protected by copyright. If the photographs are still under copyright protection, the specialist must obtain permission from the copyright holder or ensure that their use falls under fair use or another exception to copyright law.

Practical Application: Digital preservation specialists often work with a wide range of digital content, including text, images, audio, video, and software. Understanding copyright and intellectual property rights is essential for managing these materials effectively. Specialists must be able to identify the rights associated with each type of content and ensure that they comply with legal requirements when preserving and providing access to digital collections.

Challenges: One of the main challenges in managing digital collections is navigating the complex legal landscape surrounding copyright and intellectual property rights. The laws governing these rights can vary by jurisdiction and are subject to interpretation by courts. Digital preservation specialists must stay up-to-date on changes in copyright law and be prepared to address any legal issues that may arise when managing digital collections. Additionally, the proliferation of digital content has made it increasingly difficult to identify and locate copyright holders, posing a significant challenge for specialists seeking permission to preserve and provide access to digital materials.

Copyright and Intellectual Property Rights

Copyright

Copyright refers to a legal right that grants the creator of an original work exclusive rights to its use and distribution. This includes the right to reproduce, distribute, and display the work. Copyright protection applies to various forms of creative works, such as literary works, music, art, software, and more. Copyright is automatically granted to the creator upon the creation of the work, providing them with control over how their work is used.

Intellectual Property Rights (IPR)

Intellectual Property Rights (IPR) refer to the rights granted to individuals or organizations for their intellectual creations, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce. These rights include copyright, patents, trademarks, and trade secrets. IPR are essential for protecting the creations of individuals or organizations and encouraging innovation and creativity.

Public Domain

Public domain refers to works that are not protected by copyright law or whose copyright has expired. Works in the public domain can be freely used by anyone without obtaining permission from the creator. Examples of works in the public domain include old folk tales, historical documents, and works where the copyright has expired.

Fair Use

Fair use is a legal doctrine that allows the limited use of copyrighted material without obtaining permission from the copyright owner. This doctrine is based on the belief that certain uses of copyrighted material are beneficial to society, such as criticism, commentary, news reporting, teaching, and research. Fair use is determined on a case-by-case basis and considers factors such as the purpose of the use, the nature of the copyrighted work, the amount used, and the effect on the market value of the work.

Intellectual Property (IP)

Intellectual Property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce. IP is protected by law through patents, copyrights, trademarks, and trade secrets. IP rights enable creators to control and benefit from their creations and encourage innovation and creativity.

Derivative Work

A derivative work is a new work that is based on or derived from an existing copyrighted work. This can

include adaptations, translations, sequels, and other modifications of the original work. In order to create a derivative work, the creator must obtain permission from the copyright owner of the original work.

Plagiarism

Plagiarism is the act of using someone else's work or ideas without giving proper credit to the original creator. This includes copying and pasting text, images, or ideas without permission or citation. Plagiarism is a serious ethical and legal offense that can result in consequences such as academic penalties, legal action, and damage to one's reputation.

Public Performance Rights

Public performance rights refer to the legal rights granted to copyright owners to control the public performance of their works. This includes performances of music, movies, theater productions, and other creative works in public spaces. Public performance rights are essential for ensuring that creators are compensated for the use of their works in public settings.

Work for Hire

Work for hire refers to a legal arrangement in which the creator of a work is hired or commissioned to create a specific work for someone else. In a work for hire agreement, the copyright of the work belongs to the employer or the person who commissioned the work, rather than the creator. This is common in situations where a company hires a freelance artist or writer to create content for them.

Copyright Duration

Copyright duration refers to the length of time that copyright protection lasts for a work. The duration of copyright protection varies depending on the type of work and the country in which it was created. In general, copyright protection lasts for the life of the creator plus a certain number of years after their death. After the copyright duration expires, the work enters the public domain and can be freely used by anyone.

Orphan Works

Orphan works are copyrighted works for which the copyright owner is unknown or cannot be located. This can happen when the creator has died, the work was created by an organization that no longer exists, or the creator has abandoned the work. Orphan works present challenges for organizations and individuals who want to use the works but cannot obtain permission from the copyright owner.

Digital Rights Management (DRM)

Digital Rights Management (DRM) refers to technologies and strategies used to protect digital content from unauthorized use and distribution. DRM systems can include encryption, watermarking, access controls, and digital locks to prevent piracy and ensure that creators are compensated for their work. DRM is often used in digital media such as e-books, music, movies, and software.

Creative Commons

Creative Commons is a nonprofit organization that provides free licenses for creators to share their work with the public while retaining certain rights. Creative Commons licenses allow creators to specify how their work can be used, shared, and modified by others. There are several types of Creative Commons licenses, each with different permissions and restrictions, such as allowing commercial use, requiring attribution, or

prohibiting derivative works.

Open Access

Open Access refers to the practice of providing free, immediate, online access to scholarly research and other works. Open Access allows researchers, students, and the public to access and use academic and scientific information without barriers such as paywalls or copyright restrictions. Open Access promotes the dissemination of knowledge and supports innovation and collaboration in research.

Digital Preservation

Digital Preservation is the practice of ensuring that digital information remains accessible and usable over time. This includes strategies and techniques for preserving digital content, such as documents, images, videos, and software, to prevent loss, degradation, or obsolescence. Digital Preservation is essential for maintaining the integrity and authenticity of digital materials for future generations.

Metadata

Metadata is data that provides information about other data. In digital preservation, metadata describes the characteristics and context of digital objects, such as their creator, creation date, file format, and usage rights. Metadata is essential for managing and preserving digital content, enabling users to search, discover, and access digital materials effectively.

Preservation Metadata

Preservation Metadata is metadata that describes the preservation aspects of digital objects, such as their provenance, authenticity, and fixity. Preservation metadata is used to ensure the long-term viability of digital materials by documenting their preservation history, actions taken to maintain them, and any changes or alterations that have occurred. Preservation metadata is crucial for digital preservation efforts.

Format Migration

Format Migration is the process of converting digital content from one file format to another to ensure its continued accessibility and usability. Format migration is necessary to address obsolescence and technological changes that may render digital content unreadable or unusable. By migrating digital content to current, supported formats, organizations can preserve their digital materials for the long term.

Bit Rot

Bit Rot refers to the gradual decay or corruption of digital data over time due to factors such as hardware failure, software obsolescence, or storage media deterioration. Bit Rot can result in the loss or corruption of digital materials, making them inaccessible or unusable. To prevent Bit Rot, organizations must implement robust digital preservation strategies, including regular backups, format migration, and data integrity checks.

Trusted Digital Repository

A Trusted Digital Repository is an organization that has been certified to store, manage, and preserve digital materials over the long term. Trusted Digital Repositories adhere to best practices and standards for digital preservation, such as the OAIS (Open Archival Information System) reference model, and undergo regular audits to ensure the integrity and authenticity of their digital collections. Trusted Digital Repositories are

essential for ensuring the long-term accessibility and usability of digital materials.

OAIS (Open Archival Information System)

The OAIS (Open Archival Information System) is a reference model that defines the functional components and responsibilities of a digital archive or repository. The OAIS model provides a framework for preserving and managing digital information over time, including ingest, storage, data management, access, and preservation planning. Organizations that follow the OAIS model can ensure the integrity, authenticity, and long-term viability of their digital collections.

Checksum

A checksum is a unique value computed from digital data to verify its integrity and detect errors or corruption. Checksums are commonly used in digital preservation to ensure that data has not been altered or damaged during storage, transfer, or processing. By comparing checksum values before and after data manipulation, organizations can confirm the integrity of their digital materials and detect any discrepancies that may indicate data loss or corruption.

Emulation

Emulation is a digital preservation strategy that involves running obsolete software and hardware on modern systems to access and use legacy digital content. Emulation allows organizations to overcome obsolescence and technological challenges by recreating the original computing environment in which digital materials were created. Emulation is used to preserve and access legacy software, games, and other digital content that may no longer be supported by current technologies.

Web Archiving

Web Archiving is the process of collecting, preserving, and providing access to web content for future use. Web archiving involves capturing and storing websites, social media, online publications, and other digital content to document the evolution of the web and preserve cultural, social, and historical information. Web archiving tools and services are used by libraries, archives, and cultural heritage institutions to create web archives and ensure the long-term accessibility of online content.

Dark Archives

Dark Archives are secure, offline storage facilities used to store digital materials that are not intended for immediate access or use. Dark archives are kept disconnected from the internet and other networks to protect sensitive or valuable digital content from cyber threats, data breaches, and unauthorized access. Dark archives are used to preserve critical digital materials, such as legal documents, research data, and sensitive information, in a secure and protected environment.

Digital Forensics

Digital Forensics is the practice of collecting, analyzing, and preserving digital evidence for investigative or legal purposes. Digital forensics involves examining digital devices, networks, and data to uncover evidence of cybercrime, data breaches, or unauthorized activities. Digital forensics tools and techniques are used by law enforcement agencies, cybersecurity professionals, and legal experts to investigate and prosecute digital crimes and ensure the integrity of digital evidence.

Born-Digital

Born-Digital refers to digital materials that are created in a digital format, rather than being digitized from analog sources. Born-digital materials include documents, photos, videos, and other content that are born in a digital form and exist only in digital form. Born-digital materials present unique challenges for digital preservation, as they require specialized strategies and technologies to ensure their long-term accessibility and usability.

Digitization

Digitization is the process of converting analog materials, such as physical documents, photographs, and audio recordings, into digital format. Digitization involves scanning, capturing, and encoding analog content into digital files for preservation, access, and sharing. Digitization is used to convert historical, cultural, and scientific materials into digital form to ensure their long-term preservation and accessibility.

Lock-in

Lock-in refers to a situation in which an organization becomes dependent on a particular technology, software, or service provider, making it difficult or costly to switch to alternatives. Lock-in can limit the organization's flexibility, innovation, and ability to adapt to changing needs or requirements. To avoid lock-in, organizations should consider interoperable, open-source, and standards-based solutions for digital preservation to ensure long-term sustainability and flexibility.

Migration

Migration is the process of transferring digital content from one storage system, platform, or format to another to ensure its continued accessibility and usability. Migration may be necessary to address technological obsolescence, hardware failures, or changes in software or file formats. By migrating digital content to current, supported technologies, organizations can preserve their digital materials and prevent loss or degradation over time.

Metadata Schema

A Metadata Schema is a structured framework for organizing and describing metadata elements to facilitate the management and discovery of digital content. Metadata schemas define the types of metadata that can be captured, their relationships, and the rules for their use. Common metadata schemas used in digital preservation include Dublin Core, PREMIS (Preservation Metadata: Implementation Strategies), and METS (Metadata Encoding and Transmission Standard).

Format Obsolescence

Format Obsolescence refers to the situation where a digital file format becomes outdated, unsupported, or incompatible with current technologies, making it difficult or impossible to access or use digital content. Format obsolescence can lead to the loss or degradation of digital materials, rendering them inaccessible or unusable. To address format obsolescence, organizations should monitor and plan for the preservation of digital content in sustainable, open, and widely supported formats.

Bitstream Preservation

Bitstream Preservation refers to the long-term storage and maintenance of digital files in their original form, without alteration or conversion. Bitstream preservation ensures that the exact binary representation of

digital content is preserved over time, allowing for future access, migration, and emulation. Bitstream preservation is essential for maintaining the authenticity and integrity of digital materials and ensuring their continued usability.

Legal Deposit

Legal Deposit is a legal requirement for publishers, authors, and creators to deposit copies of their publications or works with designated national libraries or archives. Legal deposit ensures the preservation and accessibility of published materials for future generations, researchers, and the public. Legal deposit laws vary by country and may include printed materials, digital publications, audiovisual media, and online content.

Access Restrictions

Access Restrictions are limitations placed on the use, sharing, or distribution of digital content to protect privacy, intellectual property rights, or sensitive information. Access restrictions may include password protection, encryption, licensing agreements, and digital rights management (DRM) to control who can access, use, or modify digital materials. Access restrictions are important for safeguarding digital content and ensuring compliance with legal and ethical requirements.

Versioning

Versioning is the practice of creating and managing multiple versions or iterations of digital content to track changes, updates, and revisions over time. Versioning allows organizations to preserve a history of changes to digital materials, compare different versions, and revert to previous versions if needed. Versioning is commonly used in collaborative editing, software development, and content management systems to maintain the integrity and accuracy of digital content.

Digital Curation

Digital Curation is the practice of collecting, organizing, preserving, and providing access to digital materials to ensure their long-term usability and value. Digital curation involves selecting, describing, and managing digital content, applying metadata, and preserving digital materials for future use. Digital curators play a critical role in digital preservation by ensuring that digital collections are well-maintained, accessible, and sustainable over time.

Rights Management

Rights Management refers to the process of managing and enforcing intellectual property rights, licensing agreements, and access permissions for digital content. Rights management systems are used to track, control, and monetize the use of digital materials, such as music, images, videos, and software. Rights management is essential for ensuring that creators are properly compensated for their work and that users comply with copyright laws and licensing terms.

Intellectual Property Infringement

Intellectual Property Infringement occurs when someone violates the intellectual property rights of a creator by using, copying, or distributing their work without permission. Intellectual property infringement includes copyright infringement, trademark infringement, patent infringement, and other violations of IP rights. Intellectual property infringement can result in legal action, fines, damages, and loss of reputation for the

infringing party.

Digitization Standards

Digitization Standards are guidelines and specifications for converting analog materials into digital format to ensure quality, accuracy, and interoperability. Digitization standards define best practices for scanning, encoding, and preserving digital content, such as resolution, file formats, metadata requirements, and quality control measures. Adhering to digitization standards helps organizations create high-quality digital collections that are sustainable, accessible, and compatible with digital preservation practices.

Preservation Planning

Preservation Planning is the process of developing strategies, policies, and workflows to ensure the long-term preservation and accessibility of digital materials. Preservation planning involves assessing risks, setting priorities, allocating resources, and implementing preservation actions to protect digital content from loss, degradation, or obsolescence. Preservation planning is essential for organizations to sustainably manage their digital collections and ensure their continued usability for future generations.

Disaster Recovery

Disaster Recovery is the process of restoring and recovering digital materials after a catastrophic event, such as a natural disaster, cyberattack, hardware failure, or data breach. Disaster recovery plans include backup procedures, data recovery strategies, and contingency measures to minimize data loss and restore operations in the event of a disaster. Disaster recovery is crucial for protecting digital collections and ensuring business continuity in the face of unforeseen emergencies.

Open Source Software

Open Source Software is software that is freely available for use, modification, and distribution by anyone under an open-source license. Open source software promotes collaboration, innovation, and transparency by allowing users to access, modify, and share the source code. Open source software is commonly used in digital preservation for tools, platforms, and systems that support the long-term accessibility and sustainability of digital materials.

Interoperability

Interoperability is the ability of different systems, software, or devices to exchange and use information effectively. Interoperability ensures that digital content can be accessed, shared, and preserved across various platforms, formats, and technologies. Interoperability is essential for digital preservation to enable the seamless transfer, migration, and integration of digital materials while maintaining their integrity and usability over time.

Preservation Policy

Preservation Policy is a set of guidelines, procedures, and principles that govern the management and preservation of digital materials within an organization. Preservation policies outline the goals, responsibilities, workflows, and best practices for preserving digital content, including selection criteria, metadata standards, access restrictions, and preservation strategies. Preservation policies help organizations ensure the long-term sustainability and accessibility of their digital collections.

Risk Assessment

Risk Assessment is the process of identifying, analyzing, and evaluating potential risks and threats to digital materials and the systems that store and manage them. Risk assessment helps organizations understand vulnerabilities, prioritize mitigation strategies, and implement safeguards to protect digital content from loss, corruption, or unauthorized access. Risk assessment is an essential component of digital preservation planning to ensure the security, integrity, and longevity of digital collections.

Community Engagement

Community Engagement involves building relationships, collaborating, and sharing knowledge with stakeholders, users, and partners to support digital preservation initiatives. Community engagement fosters awareness, participation, and support for digital preservation efforts by involving diverse perspectives, expertise, and resources. Community engagement can take various forms, such as outreach events, training programs, user feedback, and collaborative projects, to promote the value and impact of digital preservation within the community.

Preservation Metadata Schema

Preservation Metadata Schema is a structured framework for describing and managing metadata that is essential for preserving digital materials. Preservation metadata schemas define the elements, relationships, and standards for capturing information about the preservation status, history, and actions taken to maintain digital content. Common preservation metadata schemas

Copyright and Intellectual Property Rights

Copyright and Intellectual Property Rights are crucial concepts in the digital preservation field, governing the ownership and usage rights of digital content. Understanding these terms is essential for digital preservation specialists to ensure compliance with legal frameworks and protect valuable digital assets.

Copyright

Copyright is a legal concept that grants creators the exclusive rights to their original works, such as literary, artistic, musical, and digital creations. It provides creators with the right to control how their works are used, distributed, and reproduced. Copyright protection is automatic upon the creation of a work and typically lasts for the life of the creator plus an additional 70 years.

Related Terms: Fair Use, Public Domain, Copyright Infringement

Example: An artist retains the copyright to their digital artwork, allowing them to license its use to others for commercial purposes.

Intellectual Property Rights

Intellectual Property Rights (IPR) encompass a broader range of legal rights that protect intangible creations, including copyrights, patents, trademarks, and trade secrets. IPR ensure that creators and innovators are rewarded for their efforts and have the exclusive rights to exploit their creations for a specified period.

Related Terms: Patent, Trademark, Trade Secret

Example: A software company holds intellectual property rights to its proprietary code, preventing competitors from copying or using it without permission.

Fair Use

Fair Use is a legal doctrine that allows limited use of copyrighted material without permission from the copyright owner for purposes such as criticism, commentary, news reporting, teaching, scholarship, or research. Fair Use is determined by factors such as the purpose of the use, the nature of the copyrighted work, the amount used, and the effect on the market value of the original work.

Related Terms: Transformative Use, Parody, Copyright Exceptions

Example: A researcher can quote excerpts from a copyrighted book in their academic paper under Fair Use guidelines.

Public Domain

Public Domain refers to works that are not protected by copyright and are freely available for anyone to use, modify, and distribute. Works enter the public domain when their copyright expires, the creator relinquishes their rights, or the work lacks sufficient originality to qualify for copyright protection.

Related Terms: Creative Commons, Orphan Works, Copyright Term

Example: The works of William Shakespeare are in the public domain, allowing anyone to freely perform, publish, or adapt his plays without permission.

Copyright Infringement

Copyright Infringement occurs when someone uses, reproduces, distributes, or displays copyrighted material without permission from the copyright owner. Infringing on copyright rights can result in legal consequences, such as fines, damages, and injunctions. Digital technologies have made it easier to detect and enforce copyright infringement online.

Related Terms: DMCA, Cease and Desist, Piracy

Example: A website streaming movies without the rights to distribute them is committing copyright infringement.

DMCA

The Digital Millennium Copyright Act (DMCA) is a U.S. law that addresses copyright issues related to digital content and the internet. The DMCA provides a framework for copyright owners to protect their works online, including provisions for takedown notices, safe harbor for internet service providers, and anti-circumvention measures.

Related Terms: Takedown Notice, Safe Harbor, Anti-Circumvention

Example: A music label issues a DMCA takedown notice to a website hosting unauthorized copies of its songs.

Plagiarism

Plagiarism is the act of using someone else's work, ideas, or expressions without proper attribution or permission, presenting them as one's own. Plagiarism is a serious ethical violation and can have academic, professional, and legal consequences. Digital tools make it easier to detect and prevent plagiarism in digital content.

Related Terms: Academic Integrity, Citation, Self-Plagiarism

Example: A student copies paragraphs from a website into their research paper without citing the source, committing plagiarism.

Creative Commons

Creative Commons is a nonprofit organization that provides a set of licenses for creators to share their work with varying levels of permissions and restrictions. Creative Commons licenses allow creators to specify how others can use, modify, and distribute their works while retaining certain rights. These licenses promote collaboration, sharing, and reuse of creative content.

Related Terms: Attribution, ShareAlike, NonCommercial

Example: A photographer releases their images under a Creative Commons license, allowing others to use them for non-commercial purposes with proper attribution.

Orphan Works

Orphan Works are copyrighted works whose owners are unknown or cannot be located, making it difficult or impossible to obtain permission to use the works. Orphan works pose challenges for digital preservationists and cultural institutions seeking to digitize and provide access to these materials. Some countries have enacted legislation to address the use of orphan works under certain conditions.

Related Terms: Copyright Clearance, Due Diligence, Risk Assessment

Example: A museum wants to digitize a collection of photographs, but the copyright owners are unknown, creating a dilemma of how to proceed with the project.

Trademark

A Trademark is a distinctive sign, symbol, or logo used to identify and distinguish the goods or services of one business from those of others. Trademarks help consumers recognize and associate products with specific brands, ensuring consistency and quality. Trademark protection prevents others from using similar marks that could cause confusion in the marketplace.

Related Terms: Branding, Logo, Trademark Infringement

Example: The Nike "swoosh" logo is a trademark that distinguishes its athletic apparel and footwear from competitors' products.

Patent

A Patent is a legal right granted to inventors that gives them exclusive control over their inventions for a specified period. Patents protect novel and non-obvious inventions, processes, and designs, preventing others from using, making, or selling the patented inventions without permission. Patents encourage innovation by rewarding inventors with exclusive rights.

Related Terms: Utility Patent, Design Patent, Patent Infringement

Example: A pharmaceutical company obtains a patent for a new drug formulation, allowing them to be the sole manufacturer and seller of the medication for a set period.

Trade Secret

A Trade Secret is confidential information that provides a competitive advantage to a business, such as formulas, processes, customer lists, or software algorithms. Trade secrets are not publicly disclosed and are protected by law as long as they remain confidential. Trade secret protection requires reasonable efforts to maintain secrecy and prevent unauthorized disclosure.

Related Terms: Non-Disclosure Agreement, Confidentiality, Economic Espionage

Example: The recipe for Coca-Cola is a closely guarded trade secret that has been kept confidential for over a century.

Digital Rights Management (DRM)

Digital Rights Management (DRM) is a technology that controls access to digital content and enforces usage restrictions to protect copyright holders' rights. DRM systems encrypt content to prevent unauthorized copying, distribution, and modification. While DRM can deter piracy, it also raises concerns about consumer rights, interoperability, and fair use.

Related Terms: Encryption, License Management, Content Protection

Example: An e-book retailer uses DRM to limit the number of devices on which a purchased book can be read to prevent unauthorized sharing.

Open Access

Open Access refers to the practice of making scholarly research and publications freely available online to the public without cost or access barriers. Open Access promotes the dissemination of knowledge, accelerates research progress, and increases the visibility and impact of scholarly work. Various models, such as Green and Gold Open Access, support different approaches to providing open access to research

outputs.

Related Terms: Institutional Repository, Creative Commons, Scholarly Communication

Example: A university library supports Open Access initiatives by hosting an institutional repository of faculty publications for public access.

Data Privacy

Data Privacy refers to the protection of individuals' personal information and data from unauthorized access, use, or disclosure. Data privacy regulations and practices aim to safeguard sensitive data, such as personal identifiers, financial information, and health records, from misuse and exploitation. Digital preservationists must consider data privacy implications when handling and sharing digital collections containing personal data.

Related Terms: GDPR, Data Protection, Privacy Policy

Example: A healthcare organization implements strict data privacy measures to ensure patient confidentiality and compliance with privacy regulations.

Metadata

Metadata is descriptive information that provides context and structure to digital content, facilitating its organization, discovery, and management. Metadata includes details such as title, author, date, format, and keywords, enhancing the accessibility and usability of digital assets. Effective metadata practices are essential for digital preservation to ensure long-term access and understanding of digital collections.

Related Terms: Dublin Core, Preservation Metadata, Linked Data

Example: A digital image is accompanied by metadata that includes the photographer's name, location, date taken, and keywords for searchability.

Preservation Metadata

Preservation Metadata is specialized metadata that captures essential information about the long-term preservation of digital objects, such as file format, fixity checks, provenance, and rights management. Preservation metadata ensures the integrity, authenticity, and usability of digital materials over time, guiding preservation actions and decision-making. Adopting standardized preservation metadata schemas enhances interoperability and sustainability in digital preservation efforts.

Related Terms: PREMIS, METS, OAIS

Example: A digital archive includes preservation metadata in its records to track the provenance and format migration of its digital collections.

Digital Obsolescence

Digital Obsolescence refers to the risk of digital materials becoming inaccessible or unusable due to technological changes, hardware and software failures, or format obsolescence. Digital obsolescence poses challenges for digital preservation efforts, requiring strategies such as format migration, emulation, and refreshing to ensure continued access to digital content. Proactive planning and monitoring are essential to mitigate the impact of digital obsolescence on digital collections.

Related Terms: Format Migration, Emulation, Bit Rot

Example: A museum's digital video collection is at risk of digital obsolescence as the proprietary video format used becomes unsupported by modern players.

Format Migration

Format Migration is the process of converting digital content from one file format to another to ensure its continued accessibility and usability over time. Format migration addresses challenges such as format obsolescence, software dependencies, and technological changes that can render digital materials obsolete. Preservation standards and best practices guide format migration activities in digital preservation workflows.

Related Terms: Preservation Master, Migration Path, File Conversion

Example: A digital archive migrates its audio recordings from a legacy format to a standardized preservation format to ensure long-term access and compatibility.

Emulation

Emulation is a digital preservation strategy that replicates the original hardware and software environment needed to access and run obsolete or legacy digital content. Emulation allows obsolete software applications or operating systems to be executed on modern systems, preserving access to historical digital materials. Emulation requires emulation software, hardware, and documentation to recreate the original computing environment accurately.

Related Terms: Virtualization, Legacy Systems, Software Preservation

Example: A library uses emulation software to run vintage computer games on modern hardware for educational and research purposes.

Bit Rot

Bit Rot, also known as Data Degradation, refers to the phenomenon of data loss or corruption in digital files over time due to hardware decay, file format obsolescence, or storage media deterioration. Bit rot can result in the loss of valuable digital content if not detected and addressed promptly. Regular integrity checks, data validation, and preservation strategies help prevent bit rot and ensure the long-term viability of digital collections.

Related Terms: Data Integrity, Error Correction, Digital Preservation Risk

Example: A digital archive discovers corrupted files in its collection due to bit rot, prompting immediate action to restore and preserve the affected materials.

Digital Curation

Digital Curation is the management and preservation of digital assets over their lifecycle, including selection, acquisition, appraisal, arrangement, description, and access. Digital curation ensures the long-term usability, integrity, and authenticity of digital content for current and future users. Curation activities involve metadata creation, quality control, rights management, and preservation planning to support sustainable digital collections.

Related Terms: Digital Repository, Curatorial Practices, Lifecycle Management

Example: A digital librarian curates a collection of born-digital photographs, applying metadata standards and preservation strategies to ensure their accessibility and longevity.

Digital Repository

A Digital Repository is a managed storage system that provides access to digital assets, such as documents, images, audio, and video files, for preservation and dissemination. Digital repositories organize, store, and provide metadata for digital materials, enabling secure storage, retrieval, and sharing of digital collections. Repositories play a vital role in digital preservation by ensuring long-term access and discoverability of valuable digital resources.

Related Terms: Institutional Repository, Open Access Repository, Data Archive

Example: A university library establishes a digital repository to archive and share faculty research publications and institutional records.

Checksum

A Checksum is a unique alphanumeric value generated from a digital file's content using a mathematical algorithm, such as MD5 or SHA-256. Checksums serve as a digital fingerprint to verify the integrity and authenticity of files by comparing checksum values before and after transfer or preservation. Checksum validation detects data corruption, tampering, or errors in digital files, ensuring their reliability and accuracy.

Related Terms: Fixity Check, Data Validation, Hash Function

Example: A digital preservationist calculates and compares checksum values for audio files to confirm their integrity and prevent data loss during storage and migration.

Preservation Policy

A Preservation Policy is a formal document that outlines an organization's strategies, procedures, and responsibilities for managing and preserving digital collections. Preservation policies define preservation goals, selection criteria, formats, storage requirements, access restrictions, and disaster recovery plans to

guide preservation activities. Establishing clear preservation policies ensures consistency, transparency, and sustainability in digital preservation efforts.

Related Terms: Preservation Plan, Risk Management, Compliance

Example: A museum develops a preservation policy that specifies digitization standards, metadata schemas, and access permissions for its digital art collection.

Data Management Plan

A Data Management Plan is a structured document that describes how research data will be collected, organized, documented, stored, preserved, and shared throughout a project's lifecycle. Data management plans promote data integrity, accessibility, and reuse by detailing data workflows, metadata standards, file formats, and preservation strategies. Funding agencies and institutions often require researchers to create data management plans to ensure responsible data stewardship.

Related Terms: Data Lifecycle, Data Sharing, Data Citation

Example: A research team develops a data management plan outlining data collection methods, storage protocols, and preservation strategies for a scientific study.

Digital Forensics

Digital Forensics is the practice of collecting, analyzing, and preserving digital evidence for legal investigations and disputes. Digital forensics experts use specialized tools and techniques to recover and examine data from computers, mobile devices, networks, and storage media. Digital forensics plays a critical role in criminal investigations, cybersecurity incidents, intellectual property disputes, and e-discovery processes.

Related Terms: Chain of Custody, Electronic Discovery, Incident Response

Example: A digital forensics investigator analyzes a suspect's computer to recover deleted files and emails as evidence in a fraud case.

Open Data

Open Data refers to structured data that is freely available for anyone to access, use, and share without restrictions, subject to licensing terms. Open data initiatives aim to promote transparency, innovation, and collaboration by providing public access to government, scientific, and research data. Open data repositories and platforms support data sharing, analysis, and reuse for social, economic, and scientific benefits.

Related Terms: Data Transparency, Data Sharing, Open Government

Example: A city government publishes crime statistics as open data, allowing researchers, journalists, and the public to analyze and visualize crime trends.

Digital Preservation Risk

Digital Preservation Risk refers to potential threats and challenges that may impact the long-term viability, integrity, and accessibility of digital collections. Risks include technological obsolescence, hardware failures, data loss, security breaches, legal disputes, and funding constraints. Digital preservationists assess, prioritize, and mitigate risks through proactive planning, monitoring, and response strategies to safeguard digital assets and ensure their continued availability.

Related Terms: Risk Assessment, Mitigation Strategies, Contingency Planning

Example: A digital archive identifies hardware degradation as a high preservation risk and implements regular monitoring and maintenance to prevent data loss.

Web Archiving

Web Archiving is the process of collecting, preserving, and providing access to web content for historical, cultural, and research purposes. Web archiving captures static and dynamic web pages, social media posts, multimedia content, and online databases to document the evolving web landscape. Web archiving tools and techniques enable organizations to create comprehensive and searchable archives of web-based information.

Related Terms: Wayback Machine, Archival Crawling, Web Harvesting

Example: A national library archives websites related to significant events, elections, and social movements to preserve digital records of societal changes.

Digitization

Digitization is the process of converting analog materials, such as physical documents, images, audio recordings, and videos, into digital formats for preservation and access. Digitization involves scanning, capturing, and encoding analog content into digital files, enhancing their usability, searchability, and longevity. Digitization projects digitize cultural heritage materials, historical documents, and archival collections to ensure their digital preservation and dissemination.

Related Terms: Optical Character Recognition, Digital Imaging, Born-Digital

Example: A museum digitizes its collection of rare manuscripts to create high-resolution images for online exhibitions and research access.

Blockchain

Blockchain is a decentralized digital ledger technology that securely records transactions, contracts, and assets across a network of computers. Blockchain uses cryptographic techniques to create immutable, transparent, and tamper-proof records of data, enabling secure and verifiable transactions without intermediaries. Blockchain applications include cryptocurrency, smart contracts, supply chain management, and digital asset ownership verification.

Related Terms: Distributed Ledger, Cryptocurrency, Smart Contracts

Example: A blockchain platform enables artists to create unique digital artworks as non-fungible tokens (NFTs) that are securely owned and traded on the blockchain.

Machine Learning

Machine Learning is a branch of artificial intelligence that enables computer systems to learn from data, identify patterns, and make decisions without explicit programming. Machine learning algorithms analyze large datasets to detect trends, predict outcomes, and automate tasks, improving efficiency and accuracy. Machine learning applications in digital preservation include image recognition, text analysis, and data classification for managing and preserving digital collections.

Related Terms: Artificial Intelligence, Deep Learning, Data Mining

Example: A machine learning model classifies and tags digital photographs based on their content and context to enhance search and retrieval capabilities.

Geographic Information Systems (GIS)

Geographic Information Systems (GIS) are computer-based tools that capture, store, analyze, and visualize spatial data to understand patterns, relationships, and trends in geographic information. GIS integrates maps, satellite imagery, and geospatial data to create interactive maps, conduct spatial analysis, and solve complex geographic problems. GIS applications in digital preservation include mapping cultural heritage sites, monitoring environmental changes, and documenting historical landscapes.

Related Terms: Spatial Data, Cartography, Remote Sensing

Example: A conservation organization uses GIS to map and monitor biodiversity hotspots, deforestation trends, and wildlife habitats for conservation planning.

Artificial Intelligence (AI)