Data Security and Privacy Policy

REVISION HISTORY:

Version	Approval date	Title	Explanation on changes
V1	Jan 1st, 2022	Information Security Policy	Initial release
V2	See approval below	Data Security and Privacy Policy	V1 was updated to better align with NIST framework

APPROVAL:

Version	Approval Date	Approver Signature
V2	4/11/2023	David Kuizenga

Data Security and Privacy Policy

Table of Contents

1. Scope and Purpose

This Data Security and Privacy Policy ("Policy") is a critical component of Common Sense Media Inc., a non-profit company and affiliates ('Common Sense," "we," or "us") privacy and security program as it outlines the minimum requirements necessary to ensure the confidentiality, integrity, and availability of Information Technology (IT) assets and data. This includes all information systems and communication networks, whether owned, leased, or rented by Common Sense, and the information stored, processed, and transmitted on or by these systems and networks.

This Policy addresses Common Sense's responsibility to adopt appropriate administrative, technical, and physical safeguards and controls to protect and maintain its IT assets and data's confidentiality, integrity, and availability. In addition, these policies ensure Common Sense's adherence to applicable legal and regulatory requirements[1] and conform to best practices across the entire data and IT system lifecycle of creation, collection, retention, dissemination, protection, and destruction.

This Policy controls in the event of any conflict or inconsistency between this Policy and any other incident response policies, procedures, or related documents used at the organization level or otherwise.

Document structure:
This document is organized as follows:

- Section 1 is the introduction and introduces the policies, outlines the purpose, and establishes the implementation applicability.
- Section 2 defines the roles and responsibilities for individuals tasked to oversee and manage the Common Sense data privacy and information security program.
- Sections 3-10 provide a comprehensive privacy and cybersecurity policy statement set. The statements are organized by function and include privacy and governance, asset management, access control, awareness and training, data security, information protection, maintenance, and anomalies and events. The headings align to Common Sense's chosen cybersecurity framework – the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) categories. Where applicable, NIST CSF categories were merged, and additional requirements added to better align to the Common Sense organization and mission.

This Policy should be read by:

[1] Including, but not limited to, the required Data Security and Privacy Plan pursuant to New York's Education Law § 2-d and Section 121.6 of the Commissioner's Regulations.

All management and Common Sense personnel.

This Policy will apply to:
All Common Sense employees, interns, volunteers, consultants, and third parties who receive or have access to Common Sense IT assets or data.

2. Business Environment: Roles and Responsibilities

Common Sense has established and appointed applicable roles with the mission to coordinate, develop, implement, and maintain the data privacy and information security program. The roles listed below identify these positions and the specific activities personnel are responsible for executing. The DGG, CSO and, IRT must work with their respective teams and external partners to implement and maintain policies that protect the confidentiality, integrity and accessibility of Common Sense IT systems and data. The department leads at CSM are responsible for implementing privacy and security policies and practices into the operations of their departments and programs, including strategic planning, budget planning, and organization architecture.

2.1 Data Governance Group (DGG)

The Data Governance Group (DGG) is responsible for establishing the protection framework for managing data privacy risk and managing the collection, use and disclosure of Personal Information by establishing policies, procedures, and practices in accordance with applicable privacy laws, rules, regulations, Common Sense policies, and recommended industry practices. The DGG will coordinate the implementation of a data governance strategy. Part of the role of the DGG is to ensure that data privacy and protection activities are integrated into Common Sense's management activities, including strategic planning, capital planning, and system design and architecture.

2.2 Chief Security Officer (CSO)

The Chief Security Officer (CSO) is responsible for establishing the information security governance framework and overseeing Common Sense's implementation of information security. Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.

2.3 Incident Response Team (IRT)

Under the supervision of the CSO, the Incident Response Team (IRT) is responsible for the Incident Management Process. The goal of the IRT is to identify, review, and maintain all security, privacy, and incident related policies and controls.

3. Governance

Common Sense shall develop, implement, and maintain an organization-wide privacy and security program to address the confidentiality, integrity and accessibility of Common Sense IT

systems and data that support the operations and assets of Common Sense, including those provided or managed by another organization, contractor, or other source.

3.1 Acceptable use policy, user account password policy and other related policies

- Users must comply with Common Sense's information security policies, which outline the responsibilities of all users of Common Sense information systems to maintain the security of the systems and to safeguard the confidentiality of Common Sense information.
- Users must comply with the acceptable use of IT resources policies in using Common Sense resources.
- Users must comply with the user account password policies.
- All remote connections must be made through managed points-of-entry in accordance with the guidelines for remote work and telecommuting policies.

3.2. Data Privacy and Vendor Management

- The confidentiality of Common Sense data must be protected and must only be used in accordance with state and federal laws, rules and regulations, and Common Sense's policies to prevent unauthorized use and/or disclosure.
- The DGG leads security and privacy compliance at Common Sense. The DGG reviews, approves, and/or provides guidance to Common Sense leads and personnel when the collection, disclosure, or new processing of Personal Information protected by law is contemplated.
- Following Common Sense privacy notice, applicable law, and this Policy, Personal Information shall only be disclosed to third parties according to a written agreement that includes terms and conditions necessary to protect such information.
- Common Sense shall have in place a contracting process that ensures that its personnel and any subcontractors with access to Personal Information are bound by a written agreement that requires them, at a minimum, to abide by Common Sense contractual and legal obligations.
- Common Sense plans to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under applicable state and federal regulations, including the Children Online Privacy Protection Act, Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes.

3.3. Risk Management Strategy

- Common Sense will have policies and practices in place that identify the risks to the confidentiality, integrity, and accessibility of its IT systems and data and manage its operations and the actions of its employees and vendors to minimize, mitigate or eliminate identified risks in line with applicable laws, rules and regulations, and industry recommended practices.

- Common Sense will manage any data security and privacy incidents that implicate Personal Information following Common Sense Incident Management and Breach Response Policy and shall report any breaches and/or unauthorized disclosures to regulators and other third parties (including school districts) in compliance with its contractual and legal obligations.
- To aid the implementation of this strategy, Common Sense shall:
    - Conduct routine penetration tests to identify vulnerabilities that adversaries could exploit.
    - Develop policies, processes, and procedures to manage and monitor Common Sense's compliance with regulatory, legislative, technical, and organizational mandates that protect data confidentiality, integrity, and availability.
    - Address data privacy requirements and compliance by third-party vendors through its contracting process and must include terms and provisions in its contracts that address the risks to Common Sense IT systems and data.
    - Adopt policies and processes to ensure risks to data are identified, assessed, and responded to timely. Establish a process to ensure that applicable policies and procedures that address data protection are reviewed annually for improvements and updates/changes in regulations.
- The risk management strategy must be implemented consistently across Common Sense and must be periodically reviewed and updated, as required, to address organizational changes.

3.4. Risk Assessments

- Whenever there is a significant change to Common Sense's information system or environment of operation, when new systems are implemented, when major modifications are undertaken, when changes in data elements occur, or when a system is migrating or deployed to a third party or to the cloud, Common Sense will perform a risk assessment that assesses impact on privacy of Personal Information and impact to data security to assess the risk to the privacy of Personal Information of such changes.
- The risk assessment must capture the data flow (e.g., where the data is coming from, where it is processed/stored, and whom it is shared with). In addition, the risk assessment must state the legal requirement related to the collection of the data, and records retention schedule covering how long the data must be stored in the information system.
- Risk assessment results must be formally documented and disseminated to appropriate personnel including the system owner, the CSO, DGG, and other stakeholders, as applicable.

4. Asset Management

Common Sense IT assets deemed critical for Common Sense to achieve its mission and objectives must be identified and managed commensurate with their risk level and importance to the organization.

4.1. Physical Device Inventory

- All physical information systems within Common Sense shall be inventoried, and essential information systems identified in accordance with Common Sense's data classification policy.

4.2. Software and Applications

- All software platforms and applications within Common Sense shall be inventoried.
- Inventories must include detailed information about the installed software, including the version number and patch level.
- The software/application inventory must be updated periodically using an automated process where feasible.

4.3. Data Flow Map

- An inventory of the types of restricted and confidential data that Common Sense collects, where it is stored, and the third parties that receive or access it must be maintained. The inventory must document the restricted or confidential data collected, the authorization and purpose of collection and external parties to whom it is disclosed, and the authorization and purpose for such disclosure.

5. Identity Management, Authentication, and Access Controls

- Access controls shall be implemented on all Common Sense physical and virtual information systems and assets maintained by Common Sense or on behalf of Common Sense, to protect against unauthorized information alteration, loss, denial of service, or disclosure, as outlined in the information security policy.
- Common Sense must establish processes and procedures to ensure that data is protected and only those with a need to know or need to access to perform their duties and/or administrative functions can access the data. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with Common Sense's mission and business functions.
- These duties and/or administrative functions must be captured in the risk assessment for each respective information system that collects, maintains, uses, and/or shares Personal Information.
- Where technically feasible, users must be provided with the minimum privileges necessary to perform their job duties.

6. Awareness and Training

All Common Sense personnel, volunteers, interns, and contractors with access to Common Sense information systems and/or information must complete data privacy and security awareness training on an annual basis.

7. Data Security

To protect the confidentiality, integrity, and availability of Common Sense data residing within Common Sense's systems, data security and data privacy controls must be incorporated into all aspects of the information systems, including the communications among and with these systems and with systems external to Common Sense boundaries.

7.1. Data in Transit and at Rest

- All data in transit and at rest containing confidential or restricted information must be encrypted following the Common Sense encryption standards where technically feasible. Where encryption is not technically feasible, one or more approved compensating control(s) must be adopted that address the same risk following applicable policies, laws, regulations, and standards.
- Systems must implement cryptographic mechanisms to prevent unauthorized disclosure of data and detect changes to data during transmission where technically feasible unless otherwise protected by appropriate safeguards.
- All Common Sense laptop computers must be secured following the Common Sense encryption standards.
- Removable media must not be used to store confidential or restricted information unless the removable media are encrypted following the Common Sense encryption standards.
- Removable written media must be encrypted following the Common Sense encryption standards.

7.2. Data Minimization

Common Sense aims to reduce the severity of security and privacy risks by limiting the amount of Personal Information it processes to what is strictly necessary to achieve a defined purpose. Good practices related to this control that is considered and implemented if appropriate include:

- Justify the collection of each piece of data and confirm that the personal data are adequate, relevant, and not excessive concerning the intended purpose; otherwise, do not collect the data.
- Reduce sensitivity where possible (via conversion into a less sensitive Personal Information form or pseudonymized) and restrict access to data (e.g., limiting access to systems data according to the "need to know" principle and restrict the transmission of documents containing personal data to the individuals who need them in connection with their work.)

- Securely delete personal data that are no longer necessary or when requested by individuals from the system in operation and/or from backups where applicable (e.g., deleting yearly data stored in systems used for educational offerings and collecting anonymized data from students and teachers.)

8. Information Protection Processes and Procedures

System protection controls must be established, implemented, and enforced on all essential Common Sense information systems in accordance with Common Sense security standards.

8.1. Configuration Management

- An enterprise configuration management plan must be developed, documented, and implemented.
- Personnel with configuration management responsibilities must be trained on Common Sense's configuration management process.
- A current baseline configuration of essential systems must be developed, documented, and maintained.
    - Baseline configurations for Common Sense workstations and laptops must be established, and images must be automatically deployed.
    - Server implementations must be deployed from a common baseline image per operating system. Baseline configurations must be reviewed and updated as part of system component installations and upgrades.
- Previous versions of the baseline configuration must be retained to support rollback.

8.2. Change Control

- Proposed system changes must be reviewed and approved prior to implementation. No scheduled changes are permitted outside of the configuration management process. The results of security impact analyses must be considered as part of the change approval process.
- Changes to systems (to include security patches) must be prioritized and implemented in a manner that ensures maximum protection against IT security vulnerabilities and minimal impact on business operations**.**
- If required changes (to include patches) are not applied, an approved risk-based decision must be documented.
- Approved changes (to include patches) must be tested and validated on non-production systems prior to implementation, where technically feasible. System changes must be analyzed to determine potential security impacts prior to change implementation.

8.3. Back-ups

- Backups of critical Common Sense systems and data must be conducted. The strategy to support system and data recovery must be documented.

- Backup data to be used for disaster recovery efforts must be stored at a secure off-site location.
- The confidentiality, integrity, and availability of backup information must be protected.
- Recovery procedures must be tested at least annually to verify procedure validity, media reliability, and information integrity. The result of the testing must be documented.

8.4. Physical Environment

- Controls must be implemented to ensure the physical and environmental protection of data and systems.
- Such controls must be commensurate with the level of data being stored, transmitted, or processed in the physical location but can include emergency power shutoff, standby power, fire detection/suppression systems, environmental controls and monitoring, and physical access control and monitoring.

8.5. Data Sanitation

- All sanitization and disposal techniques must be performed in accordance with Common Sense's secure disposal standards.
- All media sanitizations must be tracked, documented, and verified.
- Sanitization procedures must be tested.
- Both electronic and hard copy media must be sanitized prior to disposal, transfer, release out of organizational control, donation, or release for reuse, using sanitization techniques and procedures as outlined in the secure disposal standards.
- Personal identifiers must be removed from Personal Information to make it anonymous before it is provided to third parties who require it for research or before it is published publicly such that the data cannot be used to identify a specific individual.

8.6. Response Planning

- Common Sense's CSO, IRT and DGG have developed an Incident Management and Breach Response Policy to guide its response to data and cybersecurity incidents. The Incident Management and Breach Response Policy must be employed when an incident occurs.
- The Incident Management and Breach Response Policy must be:
    - Reviewed at least annually and updated to address system/organization changes.
    - Communicated to staff with incident response responsibilities.
    - Protected from unauthorized disclosure or modification.

8.7. Vulnerability Management

- A vulnerability management plan for Common Sense systems and information processing environments must be developed and implemented. Systems must be scanned for

vulnerabilities and vulnerabilities must be remediated in accordance with an assessment of risk within maximum allowable timeframes.

9. Maintenance

Repairs and maintenance on all hardware and software must be controlled and performed only by approved personnel. Questions about approval will be addressed by the DGG. Security commensurate with the sensitivity level of the system data must be implemented to protect data and information systems from unauthorized access or modification.

- All maintenance activities must be approved and monitored by designated system/facility staff.
- To the extent possible, all maintenance activities must be scheduled in advance and approval granted by the impacted parties.
- All software patches and updates must only be deployed after research and testing has been conducted in a development or test environment, where such test or development environments exist. Unless no test or development environment exists, software patch and/or update testing on operational systems is prohibited.
- All systems must be reviewed on a regular basis to ensure that current patches are applied. Maintenance tools must be inspected, approved, controlled, and monitored. All media must be checked for malicious code before being introduced to the production environment.
- A process for maintenance personnel authorization must be established and a list of authorized maintenance organization/personnel must be maintained.
- Session and network connections for remote maintenance must be terminated when non-local maintenance is completed.
- Remote maintenance and diagnostic sessions must be audited, and the records reviewed by designated system/facility staff.

9.1. Protection and Monitoring

Common Sense IT assets must be adequately protected, controlled, and monitored. Security protections commensurate with the sensitivity level of the system data must be implemented to protect Common Sense IT assets from unauthorized access or modification.

9.2. Audit

- Common Sense-designated audit logs must be recorded, retained, and available for analysis by authorized personnel to identify unauthorized activity.
- Access to the management of audit functionality must be restricted to authorized personnel only.
- Where technically feasible, audit records must be correlated across different repositories and sources to gain Common Sense-wide situational awareness and enhance the ability to identify suspicious activity.
- Internal system clocks must be used to generate time stamps for audit records.
- All audit logs must be protected from unauthorized modification, access, or destruction following the sensitivity of the data stored therein.

- Audit information and tools must be protected from deletion, unauthorized access, and modification.
- Audit logs must be retained, where technically feasible, for at least 30 days.
- Audit trails capable of automatically generating and storing security audit records must be implemented on multi-user systems.

9.3. Media Protection

- All information system media (e.g., disk drives, diskettes, internal and external hard drives, portable devices, etc.), including backup media, removable media, and media containing Common Sense information and/or sensitive information, must be always secured and protected from unauthorized access.
- Access to digital and non-digital media must be restricted to appropriate personnel.
- All media, including backup media, must be stored and transmitted securely to an off-site location following applicable business continuity and disaster recovery procedures.
- System media must be physically controlled and securely stored until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

9.4. Least Functionality

- All IT systems must be configured to provide only essential capabilities.
- Servers must not be used as workstations.
- The use of high-risk functions, ports, protocols, and/or services must be prohibited or restricted, as appropriate.

9.5. Communication Protection

- Data privacy and security controls must be incorporated into all aspects of information system and communications, to protect the confidentiality, integrity, and availability of Common Sense information systems, data residing within these systems, and the communications among and with these systems, and with systems external to Common Sense.

10. Protective Technology

- Common Sense technical security solutions described in this Policy shall be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

11. Detection: Anomalies and Events, Continuous Monitoring and Detection Processes

- System controls and processes must be implemented to ensure system and data integrity (i.e., accuracy, completeness, validity, and authenticity of systems and data) is always

protected. Measures must be taken to prevent, detect, remove, and report malicious code, viruses, worms, and Trojan horses.
- Common Sense must monitor systems to detect events for indicators of potential attacks and attacks and conduct security testing, training, and monitoring activities associated with Common Sense information systems.
- Security Incidents must be tracked and documented.

11.1. Breach/Incident Response Policy

Common Sense will respond to data privacy and Security Incidents in accordance with its Incident Management and Breach Response Policy. The incident response process will determine if there is a breach.

- The Incident Management and Breach Response Policy establishes a data breach response process and creates an Incident Response Team (IRT) comprised of existing staff members to address data breaches. Together with the CSO, the IRT must assess the potential impact of the incident and develop and execute a response plan consistent with Common Sense established procedures and requirements.
- Employees must report suspected cybersecurity incidents to the Incident Management and Breach Response Policy and their immediate supervisor or manager.
- Incident notification to senior management, regulatory authorities and individuals will take place as per the Incident Management and Breach Response Policy.

Definitions and acronyms

CSO: Chief Security Officer

COPPA: Children Online Privacy Protection Act

DGG: Data Governance Group

FERPA: Family Educational Rights and Privacy Act]

IRT: Incident Response Team

IT: Information Technology

NIST: National Institute of Standards and Technology

Personal Information means any information relating to an identified or identifiable natural person (i.e., information that can identify a person AND non-identifying information that can be linked to an identifiable person)

Security Event means any actual, suspected, or threatened occurrence with the potential to adversely impact Covered Information or the systems upon which it depends.

Security Incident means a Security Event that has resulted in (a) unauthorized use, disclosure, destruction, or alteration of, or access to, Covered Information, (b) loss or theft of Covered Information, or (c) inability to access or use Covered Information for approved business purposes.

Enforcement and Exceptions

Common Sense reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when it reasonably appears necessary to protect those assets' confidentiality, integrity, availability, or functionality.

The DGG may provide exceptions to this Policy's requirements upon request in specific circumstances, provided that the exception does not compromise the security or privacy of Personal Information. Exceptions shall be temporary.

If it is determined that there is non-compliance with or a violation of this Policy, the employee(s) or contracted individual(s) may be subject to immediate disciplinary action, up to and including termination.

Policy Management

This policy will be reviewed annually by the author or designee and updated as necessary to address current business needs adequately.

eSignature Details

Signer ID:	**F9kY64LX2DzJfGu6qaxQv7RZ**
Signed by:	David Kuizenga
Sent to email:	dkuizenga@commonsense.org
IP Address:	4.53.142.138
Signed at:	Apr 11 2023, 1:16 pm PDT