OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT

Cyber Security Incident Response Plan

Prepared By:	Jennifer Davis/DPO
Effective Date:	April 2024
Last Reviewed:	

Contents

Purpose

The Oxford school district is a trusted public education provider to K-12 students in Oxford, NY. OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT stores information related to students, staff, and internal business operations, as well as manages and maintains the technical infrastructure required to house and maintain this information.

Additionally, OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT contracts with the South-Central Regional Information Center (SCRIC), and vendors of digital services and products to manage and maintain this data and infrastructure.

This Cyber Security Incident Response Plan outlines the procedures OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT.

More specifically, this plan defines the roles and responsibilities of various OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff with respect to the identification, isolation, and repair of data security breaches, outlines the timing, direction, and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT also implements practices designed to proactively reduce the risk of unauthorized access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection, and numerous other industry-standard systems.

In the event of a cyber security incident, OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff has been trained to expeditiously deal with the matter. OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff is trained on a yearly basis to recognize anomalies in the systems they regularly utilize, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized. Throughout the year the Incident Response Manager and members of the Incident Response Team are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

The availability and protection of the information resources managed by the systems we maintain are of paramount importance to our school district and will always be a core value of our organization.

Scope

This plan applies to the physical location, information systems, institutional data, and networks of OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT and any person or device that gains access to these systems or data.

Maintaining Currency

It is the responsibility of the OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT Incident Response Team (IRT), policy committee, and Board of Education to maintain and revise this policy to ensure that it is always in a ready state.

Investigation

During a Cyber Security Incident investigation, the IRM or members of the IRT will be gathering information from multiple computer systems and/or conducting interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident will be strictly confidential throughout the investigative process. All members of the Cyber Security Incident Response Team are trained in information security and data privacy best practices. At the conclusion of the investigative process, the IRM will brief District Administration on the relevant details of the incident and the investigation. During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

Affected Stakeholders

In the event the incident involves the unauthorized access or disclosure of confidential student or staff information, OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT will communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific student records, staff records, etc.). OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT does reserve the right to withhold certain information at the discretion of the IRM if that information may jeopardize current or future investigations or pose a security risk to OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT or other entities.

In the event, the incident involves information about a non-OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT district stakeholder group, such as a neighboring district or vendor partner, OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT district will take appropriate steps to notify those entities as efficiently as possible.

In the event the incident is limited to OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT systems not containing sensitive or confidential information, it will be the discretion of OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT administration and the IRM whether to share information related to the incident with outside stakeholders.

Report Management

All reports generated during an investigation along with any evidence gathered will be stored and managed by the IRM. Any physical records will be stored in the IRM's office in a locked file. Any digital records will be stored on the internal school district network in a network share only accessible by the IRM and approved District Administrators. That share will be backed up and stored in accordance with OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT's regular backup procedures. In the event past records of incidents need to be reviewed, a written request must be made to the IRM that includes the requestor, the information requested, and the reason for the request. The IRM will review the request and has the discretion to approve or deny any request. Incident summary information will always be made available by the IRM.

Definitions

Cyber Security Event

A Cyber Security Event is any observable occurrence that is an exception to the normal operation of infrastructure, systems, or services of OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District. The standard process of the Incident Response team is used for a response. Not all events become incidents.

Examples of Events

- Potential unauthorized release or access of PII
- Phishing attempt or spam (may contain links to malware)
- Malicious software detection (by endpoint protection)
- Unknown increase in network traffic
- Unexpected configuration change
- Multiple login failures to a software or system

Cyber Security Incident

A Cyber Security Incident is an event that, as assessed by the Incident Response Team, violates the policies of OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District as related to Information Security, Physical Security, or Acceptable Use; other OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT policy, standard, or code of conduct; or threatens the confidentiality, integrity or availability of the information resources we support or utilize internally, especially sensitive information whose theft or loss may be harmful to individual students, our partners or our organization.

Examples of Incidents

- Unauthorized attempts to gain access to a computer, system, or the data within
- Data theft, corruption, or unauthorized distribution
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Interference with the intended use of IT resources

Data Breach

A data incident or breach is a term that is determined by the IRT, DPO, and legal counsel when it has been verified that Personally Identifiable Information (PII) has been stolen or corrupted.

If a data incident or breach is verified, the DPO would follow the incident reporting and notification procedure.

Data Classification

In the context of information security, data classification is the classification of data based on its level of sensitivity, and the impact to the organization/district should that data be disclosed, altered, or destroyed without authorization. The

classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data should be classified into one of three sensitivity levels or classifications:

- High sensitivity data – if compromised or destroyed in an unauthorized transaction, would have a catastrophic impact on the organization/district or individuals. For example, financial records, intellectual property, and authentication data.
- Medium sensitivity data – intended for internal use only, but if compromised or destroyed, would not have a catastrophic impact on the organization/district or individuals. For example, emails and documents with no confidential data.
- Low sensitivity data – intended for public use. For example, public website content.

Incident Response Team (IRT)

The IRT is made up of experts across different fields in the organization whose charge is to navigate the organization through a Cyber Security Incident from the initial investigation to mitigation, to post-incident review. Members include an Incident Response Manager, technical hardware and networking experts, front-end software experts, communications experts, and legal experts.

Incident Response Manager (IRM)

The IRM oversees all aspects of the Cyber Security Incident, especially the IRT. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cyber Security Incident Response Plan, to keep appropriate Incident Logs throughout the incident, and to act as the key liaison between IRT experts and the organization's management team. At the conclusion of a Cyber Security Incident, the IRM will conduct a review of the incident and produce both an Incident Summary Report and a Process Improvement Plan.

Data Protection Officer (DPO)

In compliance with NYS Education Law §2-d and Part 121 of the Commissioners Regulations (§121.8), states that each educational agency shall designate a Data Protection Officer (DPO) to be responsible for the implementation of the policies and procedures required in Education Law §2-d, and to serve as the point of contact for data security and privacy for the educational agency.

Cyber Security Incident Log

The Cyber Security Incident Log will capture critical information about a Cyber Security Incident and the organization's response to that incident and should be maintained while the incident is in progress.

Incident Summary Report (ISR)

The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including how the IRT followed the procedures and whether updates are required. The template for the ISR may be seen in Appendix B.

Process Improvement Plan (PIP)

The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based on the "lessons learned" from the recently completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix C.

Incident Response Key Contacts

Incident Response Team

Incident Response Manager			
Name:	Email:	Work Phone:	Mobile Phone:
Superintendent of Schools Terrance Dougherty	tdougherty@oxac.org	607-843-2025 x4041	607-725-3187

Data Protection Officer			
Name:	Email:	Work Phone:	Mobile Phone:
Jennifer Davis	jdavis@oxac.org	607-843-2025 x3248	607-343-0087

Technical Staff			
Name:	Email:	Work Phone:	Mobile Phone:
Thomas Hansen	thansen@oxac.org	607-843-2025 x2222	607-427-4029

Communication Specialist			
Name:	Email:	Work Phone:	Mobile Phone:
Kathryn Rutz	communications@oxac.org		

*In addition to those individuals listed above, additional experts may be included on the IRT, depending upon the nature and scope of the incident. A software support expert from the team that supports the software in question will likely be necessary. These additional members will be chosen by the IRM.

Educational Agency Partners

South Central RIC			
Name:	Email:	Work Phone:	Mobile Phone:
Ashleen Speen	aspeen@btboces.org	607-427-4423	

BOCES			
Name:	Email:	Work Phone:	Mobile Phone:
Michael Rullo	rullom@dcmo.com	607-335-1233	

NYSED			
Name:	Email:	Work Phone:	Mobile Phone:
Louise Decandia	privacy@nysed.gove	518-474-0937	

Other Partners

Legal Counsel			
Name:	Email:	Work Phone:	Mobile Phone:
Wendy DeWind	wdewind@ferrarafirm.com	607-797-4839	

Law Enforcement			
Name:	Email:	Work Phone:	Mobile Phone:
NYS Intelligence Center		844-628-2478	

Cyber Security Insurance			
Name:	Email:	Work Phone:	Mobile Phone:
Mang Insurance/Dan Grady	Daniel.Grady@nbtinsurance.com	607-337-4442	

Vendor Partners

Dell

CDWG

PowerSchool

SCRIC

Clever

nVision

SCRIC Communication

Upon discovery of a cyber security incident that affects OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District's services, systems, or devices that the SCRIC supports, SCRIC personnel will initiate communication as expeditiously as possible. Depending on the severity and origin of the incident, this communication will come from a SCRIC Service Coordinator, the Data Security and Privacy Team Lead or the Incident Response Coordinator.

The OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District recognizes that not all systems procured through the SCRIC or BOCES are not directly maintained by them, but by the third-party vendor themselves. If an incident occurs with these systems, the SCRIC will be responsible for preserving communication with that third-party vendor and provide updates to the district as they arise.

It is OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT's responsibility to maintain of third-party vendor contact list of systems within the district that the SCRIC does not directly support. If an incident originates from one of these district systems, the SCRIC is not responsible for direct mitigation but will provide communication, guidance, or other technical assistance if necessary.

District Communication

Communication with parents/community members will be disseminated via the school district superintendent or designee.

Although every incident is unique, sample communications that can be used as guidelines can be found in Appendices D-I in this document.

Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that this district is aware of the issue and is addressing it, with the promise of a follow-up. Scenarios for the release of Personally Identifiable Information (PII) are as follows:

- Should the unauthorized release of student data occur, the district shall notify the parents (or eligible students) affected by the release in the most expedient way possible.

Part 121 of the Commissioner's Regulations require this notification to occur within 60 calendar days after the breach is discovered.

- Should the unauthorized release of protected staff data occur, the district shall notify the staff members affected by the release in the most expedient way possible. Part 121 of the Commissioner's Regulations require this notification to occur within 60 calendar days after the breach is discovered.

- Should the unauthorized release of student and/or protected staff data occur, the district shall notify the Chief Privacy Officer (CPO) at the New York State Education Department (NYSED) within 10 calendar days, as required by Part 121 of the Commissioner's Regulations.

- Should the release of Social Security Number, Driver's License or Non-Driver ID Number, Account Number, or Credit/Debit Card number combined with PII occur, districts should consult Section 208 of the NYS Technology Law for notification obligations (https://its.ny.gov/breach-notification-and-incident-reporting).

Updated communications will come from the *superintendent or the Incident Response Manager*. As staff receives requests from districts for information, they should pass those requests along to the Incident Response Manager.

District staff should be clearly informed by administration and the IRT what information is public and what is internal/confidential. However, district leadership should be aware that any material or information communicated to staff can and likely will be shared with the public, including the news media.

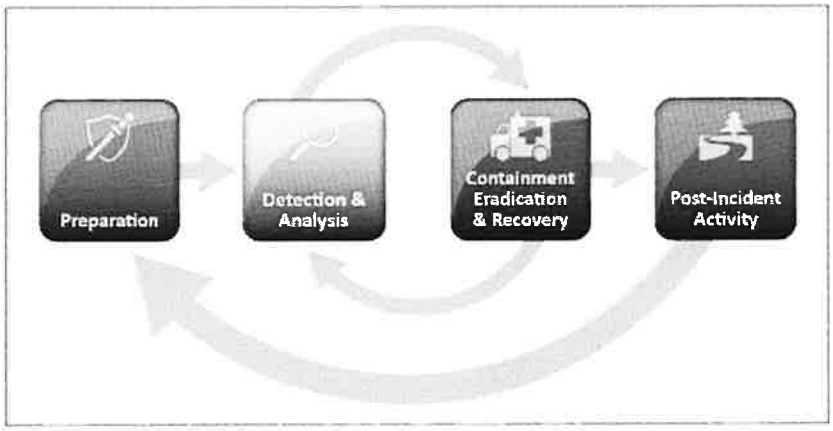
Communication with the news media will be initiated by the school district superintendent and/or designee. Incoming news media calls and requests for information will be directed through Incident Response Team Communication Specialist. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from the superintendent or designee.

Global messages, if used, should have broad language that offers basic information (1 sentence) and reassurance, and refer to separate detailed communication pieces as a follow-up.

Cyber Security Incident Response Phases

Preparation

Preparation includes those activities that enable OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT to respond to an incident.



These include a variety of policies, procedures, tools, as well as governance and communications plans.

OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT utilizes several mechanisms to prevent, and prepare to respond to, an incident using SCRIC services and technology.

- *Security Awareness Training:* All personnel are required to take annual Security Awareness Training. OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT requires annual Ed Law 2-D training, provided through RIC one, which encompasses an overview of related laws and regulations to NYS. In addition, staff are trained in general data security and privacy best practices, and ongoing threats to systems such as phishing and social engineering.
- *Malware/Antivirus/Spyware Protections*: All information system terminals, as well as key information flow points on the district network, are protected by the continuous defense against malware/antivirus/spyware and other known malicious attacks. These defense mechanisms are kept up to date without the need for end-user intervention, and end-users are restricted from accessing, modifying, disabling, or making other changes to the defense mechanisms.
- *Regional Network Protection:* Includes Wide Area Network (WAN) and district edge firewalls, redundant Internet Service Providers (ISP), Intrusion Prevention System (IPS), Vulnerability Scanning, and Distributed Denial of Service (DDoS) Protection System. For more information, please see the following link: https://drive.google.com/file/d/1HIjmxHx93m0VAS1cOzMNRZauoAbmc5Rh/view?usp=sharing
- *Physical Security Measures*: All locations within OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT that house information systems are secured. Access to these secured areas and information systems is on a need-to-know/need-to-share basis and required district-authorized access.
- *Patching/Updating:* The SCRIC performs monthly patches and updates as new security patches and hotfixes are released for the systems they support. Any software or hardware product that reaches the end of the manufacturer's service and support life for patching will be deemed out-of-compliance and replaced.
- *Contact information:* For team members and others within and outside the organization, such as law enforcement and other incident response teams; information may include phone numbers, email addresses, and instructions for verifying the contact's identity.

Incident Response Training

No incident response capability can be effectively maintained over time without proper and ongoing training. The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff will be trained on a periodic basis in procedures for reporting and handling incidents to ensure a consistent and appropriate response to an incident, and those post-incident findings are incorporated into policy and procedure.

Detection

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected cyber security event. The detection of an event being defined as an incident requires the immediate activation of the IRT. The determination of a cyber security incident can arise from one or several circumstances simultaneously.

Means by which detection can occur include:

- Trained personnel reviewing collected event data for evidence of compromise.
- Software applications analyzing events, trends, and patterns of behavior.
- Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic (SCRIC).
- The observation of suspicious or anomalous activity within an OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT facility or on a computer system.
- Report of possible unauthorized release of student or staff data.

It is critical in this phase:

- To detect whether a cyber security incident has occurred.
- To determine the method of attack.
- To determine the impact of the incident on OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT mission, systems, and stakeholders involved in the incident.

Cyber Security Event Reporting

All OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally should immediately be reported to a supervisor or the IRM if a supervisor is unavailable.

Supervisors should immediately bring the incident to the attention of the IRM. Parents are encouraged to notify the district of possible breaches or improper disclosures of data using a form on the district website (see Appendix G).

Potential cyber security events that may occur with OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff and district-issued devices that could lead to an incident are:

- Abnormal response time or non-responsiveness
- Potential unauthorized release or access of PII – Ex: Accidentally sending a document with PII to an unintended recipient that is unencrypted.
- Unexplained lockouts, content, or activity

- Locally hosted websites will not open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT staff, partners, or other actors

Analysis

Once anomalous activity has been reported, it is incumbent upon the IRT to determine the level of intervention required. Analysis of the incident indicators will be performed in a manner consistent with the type of incident. Other members of the IRT may be required to provide input during this phase to help determine if an actual security threat exists.

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been / are being / will be impacted?
- How widespread is it?
- Which stakeholders are affected?
- What kind of data might be compromised?

Documentation

The IRT will accurately document all incidents in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored in a single location so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident?
- Characteristics of the activity
- Date and time the potential incident was detected
- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the IRT is required to perform incident remediation?

Incident Response Categories

An incident will be categorized as one of three severity levels. These severity levels are based on the impact to OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to data or impact to key stakeholders. The below table provides a listing of the severity levels, their definitions, and examples of each level:

Level	Definition	Examples
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations	- Isolated virus infections - Acceptable use violations - Public-facing data compromise (press releases, district websites, district social media)

Medium	Incidents that have a significant impact, or the potential to have a severe impact, on operations	- Small-scale DDoS attack - Website compromises - Potential unauthorized access - Data that is not explicitly classified as confidential or public data such as emails and documents with no confidential data.
High	Incidents that have a severe impact on operations	- Potential compromise of sensitive data - Widespread malware attack - Unauthorized access to critical systems - DDoS affecting the entire enterprise - Confidential data (data protected by state or federal privacy regulations or protected by confidentiality agreements). For example, PII, financial records, intellectual property, and authentication data.

Response

Briefing of Administration

Upon determining that a significant cyber security incident or breach has occurred, District Administration should be notified immediately. As additional information is uncovered throughout the investigation, Administration should be briefed by the IRM so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Administration to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

Administration should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws, and the communication requirements of all parties involved. Sample communications documents may be found in Appendices D - F.

Initial Response

The first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas to define the entire scope of the incident.

Throughout this process, it will be critical to preserving all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

Containment

The Incident Response Team (IRT) is responsible for containment and will document all containment activities during an incident. Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication

The Incident Response Team (IRT) is responsible for eradication and will document all eradication activities during an incident. Eradication efforts for a security incident involve the removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery

The Incident Response Team (IRT) is responsible for recovery and will document all recovery activities during an incident. Recovery efforts for incidents will involve the restoration of affected systems to normal operation.

Once the cause has been determined and appropriately isolated, the IRT will need to remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

Reporting

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is in Appendix B. Throughout the incident, the IRT will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report.

Interviews will also be conducted with appropriate members of the IRT to obtain any additional information that may be available to augment the logs and records kept throughout the process.

Additionally, as required by Part 121 of the Commissioner's Regulations the district will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies using the login Appendix H.

Report Contents
The Incident Summary Report (ISR) will include all pertinent information to the incident, but at a minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to the discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Timeframe
The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be conducted immediately to ensure the greatest possible accuracy of information.

Post-Incident Review

The Incident Response Team (IRT) is responsible for documenting and communicating post-incident activity.

Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a cyber security incident. One of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the cyber security incident, including the incident response team.

After the conclusion of the incident, the IRM and IRT will meet with the administration to discuss the event in detail, review response procedures, and construct a Process Improvement Plan (PIP) to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented and the findings discussed. The IRM will share the full scope of the incident (as comprehensively as possible), the causes of the incident, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

Some important questions to be reviewed during this meeting are:

- Exactly what happened, and at what times?
- How well did staff and administration perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What should be done differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?

- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The group will review the information and will determine any weaknesses in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities, and what communication is required to various stakeholders.

Process Improvement Plan

The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any applicable items necessary to, prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

Incident Response Plan Procedure Resources

Appendix A: Cyber Security Incident Log

Incident Title:

Incident Opened Date:

Incident Description:

Action/Event	Details	Performed/ Reported by	Date/Time

Appendix B: Incident Summary Report (ISR)

Categories	Information
Type of Incident	
Incident Category (High/Medium/Low)	
Date Incident Originated	
Date Incident Was Detected	
By Whom Was Incident Detected	
How Was Incident Detected	
Scope of Incident (Districts / Systems Affected)	
Date Incident Corrected	
Corrective Action Types (Training, Technical, etc.)	

Summary of Incident Symptoms:

Summary of Incident Type and Scope:

Summary of Corrective Actions:

Summary of Mitigation Processes and Internal Communication:

Communications Log:

Communication Date	Communication Type	Recipient(s)	Purpose

Appendix C: Process Improvement Plan (PIP)

Areas of Success Summary:

Areas in Need of Improvement Summary:

Recommended Improvements to Avoid Future Incidents:

Recommended Improvements to the Cyber Security Incident Response Plan:

Improvement	Timeframe	Cost

Appendix D: Sample Parent Letter

DATE

Dear Parents/Guardians,

This letter is to inform you of an incident that occurred within the OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District. This incident resulted in student/staff/etc. data being compromised by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

At this time, we can share the following details:

[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

Please know that OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child's educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future.

Please contact **Jennifer Davis/DPO** with any questions you may have regarding this incident and our response.

Sincerely,

Appendix E: Sample Staff Memo

DATE

Dear Staff,

This letter is to inform you of an incident that occurred on DATE within OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT's _____ system. This incident resulted in student/staff/etc. data being compromised by an outside entity. Our response team acted quickly to assess and mitigate the situation.

I wanted to ensure that you have key details of the incident, so you are well-informed when speaking with your students and colleagues. Please note that OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT administration is handling communication with the community and affected parties. Should you receive any related inquiries, please direct them to _____.

At this time, we are able to share the following details:
[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

As more details become available, we will disseminate them as appropriate. Please contact _____ should you have any questions or immediate concerns regarding this incident.

Sincerely,

Appendix F: Sample Global Message

OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District experienced a technical issue today with its _____ system that may have resulted in **[student/staff]** data being compromised. The issue is currently under investigation. More detailed information will be distributed shortly via _____.

Appendix G: Sample Unauthorized Disclosure Complaint Form

OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District Unauthorized Disclosure Complaint Form	
Parents, eligible students (students who are at least 18 years of age or attending a postsecondary institution at any age), principals, teachers, and employees of an educational agency may file a complaint about a possible breach or improper disclosure of student data and/or protected teacher or principal data using this form. A privacy complaint may be made using this online form or by mailing the form to the OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District Data Protection Officer (DPO) at [insert district address]. After submitting the form, the DPO will promptly acknowledge receipt of the report within 24 hours. When the factfinding process is complete, the DPO will provide the reporting party with the findings made at the conclusion of the factfinding process; this should occur no later than 60 days after the receipt of the initial report, and, if additional time is needed, the reporting party shall be given a written explanation within the 60 days that includes the approximate date when the findings will be available. Please note that the OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT DPO shall maintain a record of each report received of a possible Unauthorized Disclosure or Breach, the steps taken to investigate the report, and the findings resulting from the investigation in accordance with applicable record retention policies.	
First Name:	
Last Name:	
Phone Number:	
Email:	
Role: (Student, Parent, etc.)	
Date Violation Occurred:	
Description of Data Compromised:	
Description of Improper Disclosure or Breach:	
Additional Information:	

Appendix H: Sample Unauthorized Disclosure Complaint Log

Complaint Name	**Date Complaint Submitted**
Description of Complaint	
Findings	
Date of Report made to NYSED Chief Privacy Officer (CPO)	
Date the Finding Report was Shared with Complainant	

PART 121 OF THE COMMISSIONER'S REGULATIONS REQUIREMENT
Educational agencies must maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

Educational agencies should report every discovery or report of a breach or unauthorized release of data subject to Ed Law 2-d to the Chief Privacy Officer no more than 10 calendar days after discovery.

Following its investigation, the educational agency shall also provide the parent or eligible student with a report of its findings within a reasonable period but no more than 60 calendar days from receipt of such complaint by the educational agency. In extenuating circumstances, where the educational agency requires additional time to investigate the complaint or cooperate with law enforcement, or where releasing the report may compromise security or impede the investigation of the incident, the educational agency shall provide the parent or eligible student with a written explanation that includes the approximate date when the educational agency anticipates that the report will be released.

Appendix I: Sample District Complaint Report Letter

DATE

Dear **XXXXXXX**,

On **[date complaint was submitted]** you notified OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT School District about a possible breach or improper disclosure of student data. Our Incident Response Team acted quickly to assess the situation and the report below summarizes the results of our investigation.

[insert a brief description of the complaint and findings]

OXFORD ACADEMY & CENTRAL SCHOOL DISTRICT is committed to protecting and securing educational data. Please contact _____ with any questions you may have regarding the investigation and this report.

Sincerely,