PRIVACY BREACH RESPONSE

DEFINITION

A Privacy Breach (breach) is an unauthorized disclosure, use, destruction, loss, removal, or modification of information in the custody or control of Holy Spirit Catholic School Division. Events are considered unauthorized by reference to access, privacy and security administrative procedure and/or legislation. A breach may be accidental or the result of a deliberate act.

1. **DETERMINING LEVEL OF RESPONSE**
    1. The severity of the breach determines the nature of the response reporting structure, remedial action, and the investigation process. In the response process, severity is based on:
        a. The security classification of the information, which considers potential and real harm to individuals and organizations.
        b. The internal and external scope and scale of the breach.
        c. The known relationship of the recipients to subject individuals; or
        d. The intentionality of the cause.
    2. Levels are determined when any of the designated classes and circumstances apply as indicated in Step 1 Identifying and Reporting Breach, which incorporates an assessment of the real risk of significant harm as a result of the breach.

2. INVESTIGATION PRINCIPLES

1. Holy Spirit Catholic School Division uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of persons being investigated. Investigations will, as required, incorporate the following methodologies:
    a. Keep investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;
    b. Use surveillance or monitoring data to establish past or current actions on an as-needed basis;
    c. Examine or confirm the veracity of facts or statements, sometimes using third party witnesses;
    d. Inform participants of their status and the progress of the investigation as fully and quickly as possible so long as it does not jeopardize the integrity of the investigation;
    e. Base findings and conclusions on balance of probabilities.

2. The breach investigation is an administrative rather than a disciplinary process. Once the report is delivered, it is the responsibility of Management and Human Resources to determine the appropriate disciplinary action.

PROCESSES

STEP 1: IDENTIFYING AND REPORTING BREACH

IDENTIFICATION AND REPORTING

1. When a breach level is identified, report the incident to your manager and the PAO within the Step 1 timelines in the Privacy Breach Procedures Table. If unable to determine the level of the breach, contact the PAO immediately.
2. The PAO will open and document the breach using the Privacy Breach Response Form and will document the initial facts of the breach as much as possible within the timelines available:
    a. Dates of breach and report
    b. Responsive actions taken so far
    c. Nature of the breach: unauthorized collection, use, disclosure, loss, loss of access, or modification
    d. Custody and control of the information breached
    e. Extent and scale: distribution, location and volume of information
    f. Known causes and recipients
    g. Employees, individuals and organizations involved

ASSIGNING RISK LEVEL

3. When a breach has been discovered, determine the level of the incident according to Privacy Breach Procedures Table. The highest level where any one of the classes and characteristics apply is the identified Level of the breach.

<u>Level 1 Low:</u>

Internal (I) class information:
The recipients or causes of the breach are internal (an employee or contracted service provider) or external (someone outside Holy Spirit Catholic School Division).

Confidential (C) class information:
The recipients or causes of the breach are internal only and recipients of the breached information do not know or have a relationship with any of the subject individuals involved.

The cause of the breach does not appear to be intentional.

<u>Level 2 High:</u>

Confidential (C) class information:
The recipients or causes of the breach are external, involving persons who are not employees or contracted service provider.

Confidential (C) class information:
The recipients or causes of the breach are internal and recipients of the breached information likely know or have a relationship with subject individuals involved.

Confidential (C) class information:
The cause of the breach appears to be intentional.

Restricted (R) class information
The recipients or causes of the breach are internal (an employee or contracted service provider) or external (someone outside Holy Spirit Catholic School Division).

Level 3 Critical:

Restricted (R) class information
The recipients or causes of the breach are external, involving persons who are not employees or contracted service providers.

STEP 2: CONTAINMENT AND FURTHER REPORTING

CONTAINING THE BREACH

4. At this stage, the Holy Spirit Catholic School Division uses all available means to ensure that Holy Spirit Catholic School Division information in the custody of unauthorized parties is returned to Holy Spirit Catholic School Division and/or destroyed irrevocably. If the recipient is uncooperative, this may involve legal action.

REPORTING

5. Depending on the level and nature of the breach, IT, Holy Spirit Catholic School Division leadership and the police are informed.

STEP 3: NOTIFICATION

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (OIPC) AND GOVERNMENT OF ALBERTA

6. The Holy Spirit Catholic School Division informs the Office of the Information and Privacy Commissioner of Alberta of all Level 2 or 3 breaches that involve personal information, using the OIPC online process and any process established by the Ministry of Technology and Innovation.
7. Level 1 breaches are generally not considered severe enough to pose a real risk of significant harm to an individual. However, each incident will be reviewed to confirm this status.

NOTIFICATION OF SUBJECT INDIVIDUALS

8. Holy Spirit Catholic School Division will notify identified subject individuals affected by all Level 2 or 3 breaches. Subject individuals affected by Level 1 will be notified if required by OIPC.
9. Notifications involving large numbers of subject individuals and/or individuals for which contact information is unavailable may require the use of public media.

INVESTIGATION PROCESS

10. Holy Spirit School Division will use information collected in step one and confirm the following:
    a. Dates of breach and report
    b. Responsive actions taken so far
    c. Nature of the breach: unauthorized collection, use, disclosure, loss, loss of access, or modification
    d. Custody and control of the information breached
    e. Extent and scale: distribution, location and volume of information
    f. Know causes and recipients
    g. Employees, individuals and organizations involved
11. Investigations establish facts based on evidence collected in documentation, interviews and forensics. Timelines to complete the investigation follow the standards based on level of breach in the Privacy Breach Procedures Table.

FINDINGS

12. As the outcome of the investigation, PAO will report findings on the causes, continuing risks of the breach and notification activities completed. Findings are based on a balance of probabilities determination.

REPORT DISTRIBUTION

13. If Police are investigating the breach for criminal enforcement purposes, coordinate activities with officers involved.
14. Investigative reports are distributed to Leadership and IT, HR, OIPC and the Police as required. Subject Individuals are given a summary of the findings in accordance with Holy Spirit Catholic School Division Collection, Use, Disclosure and Right of Access policies.

STEP 5: REMEDIATION AND PREVENTION

REMEDIATION

15. Remediation may have been started when immediate efforts were made to contain the breach. The investigative report will identify any further gaps or weaknesses in information security that directly or indirectly caused the breach and recommend immediate measures to close the gaps. Implementation and effectiveness of the remediation needs to be tracked.

PREVENTION RECOMMENDATIONS

16. The investigative report will identify further administrative, technical and physical security measures that can be implemented to prevent such breaches in the wider systems, processes and behaviours. This could include employee or user training, introduction of additional security technology, or upgrade to facilities.

DISCIPLINE

17. Depending on the nature and significance of the breach, the role of employees involved, and the information security administrative procedure in place, Holy Spirit Catholic School Division can take discipline action against an employee who has violated Holy Spirit Catholic School Division administrative procedures or applicable legislation. This will be passed to Leadership and Human Resources for resolution.