DATA BREACH RESPONSE PLAN POLICY

Policy document information

Policy Name	Data Breach Response Plan Policy
Supervisor	Privacy Officer
Other Policy Relationships	• Cyberspace Agreement Policy • Privacy Policy • Crisis Management and Procedure Policy • Critical Incident Report Policy • Bullying Prevention (Includes Cyber-Bullying) • Pastoral Care • Bomb Threat • Compliance Management • Emergency Evacuation Policy • Excursion,, Incursion, Camps Policy • Safety Policy – Occupational Health • School Ground Duties – Guidelines for teachers • Child Protection • Child Protection Policy –Non-Mandatory Reporting • Child Protection Policy – Mandatory reporting • Custody Arrangements/Court Orders • Reporting Policy • Criminal History Checks • Children with Special Needs/Disabilities • Fire Management, Evacuation and Lock Down • Duty of Care • Volunteers- obligations • Child Abduction Response Plan • Section 20 of the *Young Offenders Act 1994* requires the **notification of a responsible adult of the intention to question** the young person prior to questioning, unless the provisions of subsections (2) or (5) are applicable. • Surveillance in the school policy
Audience	School Board and Senior Staff members of Emmanuel Christian Community School

Key Dates

Date of issue	June, 2017
Submitted to School Board	August, 2017
Date set for review	
Date to be reviewed by the school board	

Introduction

This data breach response plan (response plan) sets out procedures and clear lines of authority for the School Board and Senior Staff of Emmanuel Christian Community School (ECCS) in the event that ECCS experiences a data breach (or suspects that a data breach has occurred).
A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.
This Data Breach Response Policy must be read together with the Cyberspace Agreement Policy. It is a requirement that every staff member must read, sign and agree to the Cyberspace Agreement Policy before using any electronic devices in the school.
This response plan is intended to enable the ECCS to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the ECCS to respond to a data breach.

Emmanuel Christian Community School shall aim to:

1. Establish a comprehensive and integrated Data Breach Response Plan and ensure that this is communicated to the whole school community and in particular to the School Board members and Senior Staff.

2. Ensure that there are appropriate organisational systems to allow prompt and effective response to a data breach situation.

3. Establish and maintain liaison with appropriate community organisations (eg. police, fire, hospital, counselling) that may be involved in a response to a data breach situation.

4. Ensure that a comprehensive training program is in place for all staff particularly those in leadership roles.

5. Ensure that all students, staff and families have appropriate support, counselling and programs available to them should a data breach event occur in the context of school activities or where such event has significant impact upon the school community.

6. Establish a Data Breach Team under the leadership of the Principal.

7. Ensure that the development of a Data Breach Response Plan follows a participative and consultative approach and addresses the four primary aspects of Prevention, Preparation, Response and Recovery.

8. Ensure the appropriate evaluation of response to any data breach, regular review and maintenance of the Data Breach Response Plan (at least annually), induction of new staff to procedures, and shall maintain an ongoing commitment to remain aware of current research and developments in this area.

9. Holding regular exercises.

THE DATA BREACH RESPONSE TEAM

It is important that tasks are designated to roles in the team, not to individuals. This will permit the plan to continue to be effective should a team member be unavailable.

1.BOARD CHAIRMAN.

The Board Chairman to use discretion in deciding whether to escalate to the response team

2. PRINCIPAL

The Principal will fulfil the role of team leader. Tasks generally associated with this role include over-seeing information dissemination to school board, Senior staff and the involvement of outside agencies.

3. DEPUTY PRINCIPAL

The Deputy Principal will take the role of the Principal in the Principal's absence and will assist the Principal in the different roles.

4. SCHOOL BURSAR

The bursar will support the team by telephone enquiries and support the coordination to ensure the continued routine functioning of the school.

5. BOARD MEMBERS

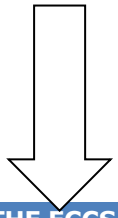
It is important that the Board members are available to assist and support.

6. SCHOOL SECRETARY

The Secretary will support the team by telephone enquiries and support to parents and students, ancillary coordination to ensure the continued routine functioning of the school.

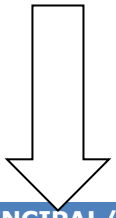
ECCS EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED

Discover by ECCS staff member or ECCS otherwise alerted



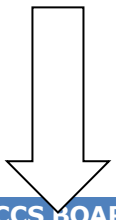
WHAT SHOULD THE ECCS STAFF MEMBER DO?

- **Immediately notify the Principal or Deputy Principal of the suspected data breach**
- **Record and advise the Principal of the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.**



WHAT SHOULD THE PRINCIPAL/DEPUTY PRINCIPAL DO?

- **Determine whether a data breach has or may have occurred.**
- **Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (Some breaches may be able to be dealt with at the Principal's level.)**
- **If so, immediately escalate to the Board Chairman.**



ALERT THE ECCS BOARD CHAIRMAN

The Board Chairman convenes the Data Breach Response Team

When should the Board Chairman escalate a data breach to the Data Breach Response Team?

The Board Chairman to use discretion in deciding whether to escalate to the response team

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (response team).
For example, a staff member may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue to the response team.
The Board Chairman should use his/her discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, The Board Chairman should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the Board Chairman to notify the response team.

The Board Chairman to inform the response team Coordinator(Principal) of minor breaches

If the Board Chairman decides not to escalate a minor data breach or suspected data breach to the response team for further action, the Board Chairman should:

• **send a brief email to the response team Coordinator(Principal)** that contains the following information:
  - description of the breach or suspected breach
  - action taken by the Board Chairman or Principal to address the breach or suspected breach
  - the outcome of that action, and
  - the Board Chairman's view that no further action is required

• **save of copy of that email in a safe place**:
Data Breach Response – reports and investigation of data breaches within the school system (internal link)

Data Breach Response Team checklist

Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

The response team should refer to Appendix 1 *Data breach notification: a guide to handling personal information security breaches* which provides further detail on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

The following checklist is intended to guide the response team in the event of a data breach, and alert the response team to a range of considerations when responding to a data breach.

STEP 1-CONTAIN THE BREACH AND DO THE PRELIMINARY ASSESSMENT	√
Convene a meeting of the data breach response team.	
Immediately contain breach: **IT to implement the *ICT Incident Response Plan* if necessary.**	
Inform the Principal and the School Board Chairman, provide ongoing updates on key developments.	
Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the Data Breach response Team to take appropriate corrective action.	
Consider developing a communications or media strategy to manage public expectations and media interest.	

STEP 2 – EVALUATE THE RISKS ASSOCIATED WITH THE BREACH	√
Conduct initial investigation, and collect information about the breach promptly, including: **□ the date, time, duration, and location of the breach** **□ the type of personal information involved in the breach** **□ how the breach was discovered and by whom** **□ the cause and extent of the breach** **□ a list of the affected individuals, or possible affected individuals** **□ the risk of serious harm to the affected individuals** **□ the risk of other harms.**	
Determine whether the context of the information is important.	
Assess priorities and risks based on what is known.	
Establish the cause and extent of the breach.	
Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.	

STEP 3 - NOTIFICATION	√
Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.	
Determine whether to notify affected individuals – is there a *real risk of serious harm to the affected individuals?* In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals.	
Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where the Data Breach Response Team is contractually required or required, by law, to notify specific parties.	

STEP 4 – REVIEW THE INCIDENT AND TAKE AC TION TO PREVENT FUTURE BREACHES	√
Fully investigate the cause of the breach.	
Report to THE Board Chairman on outcomes and recommendations: **□ Update security and response plan if necessary.** **□ Make appropriate changes to policies and procedures if necessary.** **□ Revise staff training practices if necessary.** **□ Consider the option of an audit to ensure necessary outcomes are effected.**	

Appendix 1

Data breach notification: a guide to handling personal information security breaches which provides further detail on each step.

Data breaches

How do data breaches occur?

Data breaches occur in a number of ways. Some examples include:

• lost or stolen laptops, removable storage devices, or paper records containing personal information

• hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased

• databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the ECCS

• employees accessing or disclosing personal information outside the requirements or authorisation of their employment

• paper records stolen from insecure recycling or garbage bins

• ECCS mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and

• an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

What are the reasonable steps necessary to secure personal information will depend on context, including (but not limited to):

• the sensitivity (having regard to the affected individual(s)) of the personal information held by ECCS

• the harm that is likely to result to individuals if there is a data breach involving their personal information

• the potential for harm (in terms of reputational or other damage) to ECCS if their personal information holdings are breached, and

• how ECCS stores, processes and transmits the personal information (for example, paper-based or electronic records, or by using a third party service provider).

Responding to data breaches: four key steps

Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

There are four key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and do a preliminary assessment

Step 2: Evaluate the risks associated with the breach

Step 3: Notification

Step 4: Prevent future breaches

Each of the steps is set out in further detail below.

General tips:

• Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.

• Breaches that may initially seem immaterial may be significant when their full implications are assessed.

• The decision on how to respond should be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, agencies and organisations may choose to take additional steps that are specific to the nature of the breach.

STEP 1: Contain the breach and do a preliminary assessment

Once ECCS has discovered or suspects that a data breach has occurred, it should take immediate common sense steps to limit the breach. These may include the following:

Contain the breach

Take whatever steps possible to immediately contain the breach.
For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.
Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.
For example, if it is detected that a customer's bank account has been compromised, can the affected account be immediately frozen and the funds transferred to a new account?

Initiate a preliminary assessment

Move quickly to appoint someone to lead the initial assessment. This person should have sufficient authority to conduct the initial investigation, gather any necessary information and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required.
Determine whether there is a need to assemble a team that could include representatives from appropriate parts of the school.

Consider the following preliminary questions:

- What personal information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to affected individuals) that could potentially be caused by the breach?
- How can the breach be contained?

Consider who needs to be notified immediately

Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
In some cases it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals).

Escalate the matter internally as appropriate, including informing the person or group within the agency or organisation responsible for privacy compliance.
It may also be appropriate to report such breaches to relevant internal investigation units.
If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police.
If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the Board Chairman. The Board Chairman may be able to provide guidance and assistance.

Other matters

Where a law enforcement agency is investigating the breach, consult the investigating agency before making details of the breach public.
Be careful not to destroy evidence that may be valuable in determining the cause or would allow the agency or organisation to take appropriate corrective action.
Ensure appropriate records of the suspected breach are maintained, including the steps taken to

rectify the situation and the decisions made.

STEP 2: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, agencies and organisations should assess the risks associated with the breach.
Consider the following factors in assessing the risks:

(a) The type of personal information involved.

(b) The context of the affected information and the breach.

(c) The cause and extent of the breach.

(d) The risk of serious harm to the affected individuals.

(e) The risk of other harms.

(a) Consider the type of personal information involved
Does the type of personal information that has been compromised create a greater risk of harm?

Some information is more likely to cause an individual harm if it is compromised, whether that harm is physical, financial or psychological.
For example, government-issued identifiers such as Medicare numbers, driver's licence and health care numbers, health information, and financial account numbers such as credit or debit card numbers might pose a greater risk of harm to an individual than their name or address.
Also, a combination of personal information typically creates a greater risk of harm than a single piece of personal information.
It may also matter whether the information is permanent or temporary. Permanent information, such as someone's name place and date of birth, or medical history cannot be 're-issued'.
The permanence of the information may be more significant if it is protected by encryption – over time, encryption algorithms may be broken, so such information may be at greater longer term risk of being compromised. On the other hand, temporary information may have changed by the time it has been decrypted.

Who is affected by the breach?

Employees, contractors, the public, clients, service providers, other agencies or organisations?
Remember that certain people may be particularly at risk of harm. A data breach involving name and address of a person might not always be considered high risk. However, a breach to a women's refuge database containing name and address information may expose women who attend the refuge to a violent family member. There may be less risk if the breach only relates to businesses that service the refuge.

(b) Determine the context of the affected information and the breach
What is the context of the personal information involved?

For example, a list of customers on a newspaper carrier's route may not be sensitive information. However, the same information about customers who have requested service interruption while on vacation may be more sensitive.
The sensitivity of personal information that may also publicly available information (such as the type found in a public telephone directory) also depends on context. For example, what might be the implications of someone's name and phone number or address being associated with the services offered, or the professional association represented?

What parties have gained unauthorised access to the affected information?

To whom was the information exposed? Employee records containing information about employment history such as performance and disciplinary matters or a co-worker's mental health might be

particularly sensitive if exposed to other employees in the workplace and could result in an individual being the subject of humiliation or workplace bullying.

Have there been other breaches that could have a cumulative effect?

A number of small, seemingly insignificant, breaches could have a cumulative effect. Separate breaches that might not, by themselves, be assessed as representing a real risk of serious harm to an affected individual, may meet this threshold when the cumulative effect of the breaches is considered.
This could involve incremental breaches of the same agency or organisation's database. It could also include known breaches from a number of different sources.
How could the personal information be used?

Could the information be used for fraudulent or otherwise harmful purposes, such as to cause significant embarrassment to the affected individual?
Could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

(c) Establish the cause and extent of the breach
Is there a risk of ongoing breaches or further exposure of the information?

What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?

Is there evidence of theft?

Is there evidence that suggests theft, and was the information the target? For example, where a laptop is stolen, can it be determined whether the thief specifically wanted the information on the laptop, or the laptop hardware itself?
Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as law enforcement.

Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?

Is the information rendered unreadable by security measures that protect the stored information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?
For example, if a laptop containing adequately encrypted information is stolen, but is subsequently recovered and investigations show that the information was not accessed, copied or otherwise tampered with, notification to affected individuals may not be necessary.

What was the source of the breach?

For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does the information seem to have been lost or misplaced?
The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.
For example, the client may have a common surname which leads a staff member to accidentally access the wrong client record. The access records show that the staff member immediately closed the client record once they became aware of their mistake. The risk of harm will be less in this case than in the case where a staff member intentionally and deliberately opens a client's record to browse the record, or to use or disclose that information without a legitimate business reason for doing so.

Has the personal information been recovered?

For example, has a lost laptop been found or returned? If the information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?

What steps have already been taken to mitigate the harm?

Has the agency or organisation contained the breach? For example, have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?

Is this a systemic problem or an isolated incident?

When checking the source of the breach, it is important to check whether any similar breaches have occurred in the past. Sometimes, a breach can signal a deeper problem with system security. This may also reveal that more information has been affected than initially thought, potentially heightening the awareness of the risk posed.

How many individuals are affected by the breach?

If the breach is a result of a systemic problem, there may be more people affected than first anticipated.
Even where the breach involves accidental and unintentional misuse of information, if the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The agency or organisation's response should be proportionate.
While the number of affected individuals can help gauge the severity of the breach, it is important to remember that even a breach involving the personal information of one or two people can be serious, depending on the information involved.

(d) Assess the risk of harm to the affected individuals
Who is the recipient of the information?

Is there likely to be any relationship between the unauthorised recipients and the affected individuals?
For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Was the disclosure to a person against whom the individual has a restraining order, or to co-workers who have no need to have the information?
Or was the recipient a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it? For example, was the information sent to the individual's lawyer instead of being sent to them, or to another party bound by professional duties of confidentiality or ethical standards?

What harm to individuals could result from the breach?

Examples include:

- identity theft
- financial loss
- threat to physical safety
- threat to emotional wellbeing
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships, or
- workplace or social bullying or marginalisation.

(e) Assess the risk of other harms
Other possible harms that suffered the breach

Examples include:

- the loss of public trust in the school
- reputational damage
- loss of assets (e.g., stolen computers or storage devices)
- financial exposure (e.g., if bank account details are compromised)
- regulatory penalties (e.g., for breaches of the Privacy Act)

• extortion
• legal liability, and
• breach of secrecy provisions in applicable legislation.

STEP 3: Notification
ECCS should consider the particular circumstances of the breach, and:

(a) decide whether to notify affected individuals, and, if so

(b) consider when and how notification should occur, who should make the notification, and who should be notified

(c) consider what information should be included in the notification, and

(d) consider who else (other than the affected individuals) should be notified.

Notification can be an important mitigation strategy that has the potential to benefit to the school and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. ECCS should:

• take into account the ability of the individual to take specific steps to mitigate any such harm, and
• consider whether it is appropriate to inform other third parties such as the police, or other regulators or professional bodies about the data breach.

(a) Deciding whether to notify affected individuals

The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected individual.
ECCS should consider the following factors when deciding whether notification is required:

• What is the risk of serious harm to the individual as determined by step 2?
• What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by ECCS? For example, would an individual be able to have a new bank account number issued to avoid potential financial harm resulting from a breach? Would steps such as monitoring bank statements or exercising greater vigilance over their credit reporting records assist in mitigating risks of financial or credit fraud?

• Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
• What are the legal and contractual obligations to notify, and what are the consequences of notification?

There may be adverse consequences if ECCS does not notify affected individuals. For example, if the public, including the affected individuals, subsequently find out about the breach through the media, there may be loss of public trust in ECCS (which, in turn, could have its own costs).

(b) Notification process

At this stage, ECCS should have as complete a set of facts as possible and have completed the risk assessment to determine whether to notify individuals.

Sometimes the urgency or seriousness of the breach dictates that notification should happen immediately, before having all the relevant facts.

When to notify?

In general, individuals affected by the breach should be notified as soon as reasonably possible.
If law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.
Delaying the disclosure of details about a breach of security or information systems may also be appropriate until that system has been repaired and tested or the breach contained in some other way.

How to notify?

In general, the recommended method of notification is **direct** – by phone, letter, email or in person – to the affected individuals.
Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.
Preferably, notification should be 'standalone' and should not be 'bundled' with other material unrelated to the breach, as it may confuse recipients and affect the impact of the breach notification.
In certain cases, it may be appropriate to use multiple methods of notification.

ECCS should also consider whether the method and content of notification might increase the risk of harm, such as by alerting the person who stole the laptop of the value of the information on the laptop, if it would not otherwise be apparent.
To avoid being confused with 'phishing' emails, email notifications may require special care. For example, only communicate basic information about the breach, leaving more detailed advice to other forms of communication.

Who should notify?

ECCS has a direct relationship with the customer, client or employee should notify the affected individuals.
This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate.
Joint and third party relationships can raise complex issues. For example, the breach may occur at a retail merchant but involve credit card details from numerous financial institutions, or the card promoter may not be the card issuer (for example, many airlines, department stores and other retailers have credit cards that display their brand, though the cards are issued by a bank or credit card company). Or the breach may involve information held by a third party 'cloud' data storage provider, based outside of Australia.
The issues in play in each situation will vary. ECCS will have to consider what is best on a case by case basis. However some relevant considerations might include:

- Where did the breach occur?
- Who does the individual identify as their 'relationship' manager?
- Does ECCS, that suffered the breach, have contact details for the affected individuals? Are they able to obtain them easily? Or could they draft and sign off the notification, for the lead organisation to send?

Is trust important to ECCS's activities?

Who should be notified?

Generally, it should be the individual(s) affected by the breach. However, in some cases it may be appropriate to notify the individual's guardian or authorised representative on their behalf.
There may be circumstances where carers or authorised representatives should be notified as well as, or instead of, the individual.
Where appropriate, clinical judgement may be required where notification may exacerbate health conditions, such as acute paranoia.

(c) What should be included in the notification?

The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Notifications should include the types of information detailed below:

• **Incident Description —** Information about the incident and its timing in general terms. The notice should not include information that would reveal specific system vulnerabilities.

• **Type of personal information involved —** A description of the type of personal information involved in the breach. Be careful not to include personal information in the notification, to avoid possible further unauthorised disclosure.

• **Response to the breach —** A general account of what ECCS has done to control or reduce the harm, and proposed future steps that are planned.

• **Assistance offered to affected individuals —** What ECCS will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.

For example, whether ECCS can arrange for credit monitoring or other fraud prevention tools, or provide information on how to change government issued identification numbers (such as a driver's licence number).

• **Other information sources —** Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy.

Where it is decided that a third party will notify of the breach, a clear explanation should be given as to how that third party fits into the process and who the individual should contact if they have further questions.

• **Whether breach notified to regulator or other external contact(s) —** Indicate whether ECCS has notified other parties.

• **Legal implications —** The precise wording of the notice may have legal implications; ECCS should consider whether they should seek legal advice. The legal implications could include secrecy obligations that apply to agencies.

• **How individuals can lodge a complaint with ECCS —**Provide information on internal dispute resolution processes and how the individual can make a complaint to ECCS. Refer to ECCS complaints manual and Cyberspace agreement policy.

• **How individuals can lodge a complaint with ECCS** — ECCS is covered by the Privacy Act, explain that if individuals are not satisfied with the response by ECCS to resolve the issue, they can make a complaint to the Chairman of the Board. Provide all the details that are needed.

(d) Who else should be notified?

In general, notifying the Chairman of the Board, should not be a substitute for notifying affected individuals. However, in some circumstances it may be appropriate to notify third parties:

• The following factors should be considered in deciding whether to report a breach to the Chairman of the Board or a third party:
o any applicable legislation that may require notification
o the type of the personal information involved and whether there is a **real risk of serious harm** arising from the breach, including non-monetary losses
o whether a large number of people were affected by the breach
o whether the information was fully recovered without further disclosure
o whether the affected individuals have been notified, and

o if there is a reasonable expectation that the Chairman of the Board may receive complaints or inquiries about the breach.

• **Police —** If theft or other crime is suspected, the Police should also be contacted if the breach may constitute a threat to the community.

• **Insurers or others —** If required by contractual obligations.

• **Credit card companies, financial institutions or credit reporting agencies —** If their assistance is necessary for contacting individuals or assisting with mitigating harm.

• **Other internal or external parties not already notified —** ECCS should consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards.
Consider:
o third party contractors or other parties who may be affected
o internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or
o other employee representatives.

• **Agencies that have a direct relationship with the information lost/stolen —** ECCS should consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.

STEP 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, ECCS needs to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.
A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

This plan may include:

• a security audit of both physical and technical security

• a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)

• a review of employee selection and training practices, and

• a review of service delivery partners (for example, offsite data storage providers).

The plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.
Suggested preparations for responding to a data breach include the following:

• **Develop a breach response plan** — While the aim should be to prevent breaches, having a breach response plan may assist in ensuring a quick response to breaches, and greater potential for mitigating harm.

The plan could set out contact details for appropriate staff to be notified, clarify the roles and responsibilities of staff, and document processes which will assist ECCS to contain breaches, coordinate investigations and breach notifications, and cooperate with external investigations.

• **Establish a breach response team** — consider establishing a management team responsible for responding to personal information breaches. The team could include representatives from relevant areas that may be needed to investigate an incident, conduct risk assessments and make appropriate decisions (for example, privacy, senior management, IT, public affairs, legal).

The team could convene periodically to review the breach response plan, discuss new risks and practices, or consider incidents that have occurred in other schools.

It may also be helpful to conduct 'scenario' training with team members to allow them to develop a feel for an actual breach response. Key issues to test in such training would be identifying when notification is an appropriate response, and the timing of that notification.

Identify relevant service providers — Consider researching and identifying **external** service providers that could assist in the event of a data breach, such as forensics firms, public relations firms, call center providers and notification delivery services. The contact details of the service providers could be set out in the breach response plan. This could save time and assist in responding efficiently and effectively to a data breach.

• **Enhance internal communication and training —** Ensure staff have been trained to respond to data breaches effectively, and are aware of the relevant policies and procedures. Staff should understand how to identify and report a potential data breach to the appropriate manager(s).

• **Enhance transparency** — Include information in ECCS's privacy policy about how it responds to breaches. This could include letting individuals know when and how they are likely to be notified in the event of a breach, and whether ECCS would ask them to verify any contact details or other information.
This would make clear to individuals how their personal contact information is used in the event of a breach, and may also assist individuals to avoid 'phishing' scam emails involving fake breach notifications and requests that recipients verify their account details, passwords and other personal information.

What we need to do for preventing future breaches
Some of the measures that have resulted from real-life data breaches include:

• the creation of a senior position in ECCS with specific responsibility for data security

• the institution of a ban on bulk transfers of data onto removable media without adequate security protection (such as encryption)

• disabling the download function on computers in use across ECCS, to prevent the download of data onto removable media

• the institution of a ban on the removal of unencrypted laptops and other portable devices from the school buildings

• the institution of a policy requiring the erasing of hard disk drives and other digital storage media (including digital storage integrated in other devices such as multifunction printers or photocopiers) prior to being disposed of or returning to the equipment lessor

• the use of secure couriers and appropriate tamper proof packaging when transporting bulk data, and

• the upgrading of passwords (for example, an increase from 6 to 8 characters, including numbers and punctuation), and the institution of a policy requiring passwords to be changed every 8 weeks.

Technological advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of data breaches due to the size and portability of these devices, which can be lost or misplaced more easily when taken outside of the office. There is also a risk of theft because of the value of the devices themselves (regardless of the information they contain).
Preventative steps that ECCS can take include conducting risk assessments to determine:

• whether and in what circumstances (and by which staff), personal information is permitted to be removed from the office, whether it is removed in electronic form on DVDs, USB storage devices such as memory sticks, portable computing devices such as laptops, or in paper files, and

• whether their stored data, both in the office and when removed from the office, requires security measures such as encryption and password protection.

DATA BREACH RESPONSE PROCESS

MAINTAIN INFORMATION SECURITY
Protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure. **To comply with our privacy obligation should consider:** **•the sensitivity of the personal information** **•the harm likely to flow from a security breach** **•developing a compliance and monitoring plan, and** **•regularly reviewing their information security measures**

DATA BREACH OCCURS
Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.

KEY STEPS IN RESPONDING TO A DATA BREACH		
STEP 1	Contain the breach and make a preliminary assessment	•Take immediate steps to contain breach •Designate person/team to coordinate response
STEP 2	Evaluate the risks for individuals associated with the breach	•Consider what personal information is involved •Determine whether the context of the information is important •Establish the cause and extent of the breach •Identify what is the risk of harm
STEP 3	Consider breach notification	•Risk analysis on a case-by-case basis •Not all breaches necessarily warrant notification

SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?	
Where there **is a real risk of serious harm**, notification may enable individuals to take steps to avoid or mitigate harm. Consider: •Legal/contractual obligations to notify •Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities	**Process of Notification** •**When?** - as soon as possible •**How?** - direct contact preferred (mail/phone) •**Who?** - entity with the direct relationship with the affected individual •**What?** - description of breach, type of

	personal information involved, steps to help mitigate, contact details for information and assistance.

SHOULD OTHERS BE NOTIFIED?

- **Police/Law Enforcement**
- **Professional or Regulatory Bodies**
- **Other agencies or organisations affected by the breach or contractually required to notify**

STEP 4	Review the incident and take action to prevent future breaches	•Fully investigate the cause of the breach •Consider developing a prevention plan •Option of audit to ensure plan implemented •Update security/ response plan •Make appropriate changes to policies and procedures •Revise staff training practices