*Matamata Christian School*

**PRIVACY POLICY**

(Adopted 15 October 2019)

**RATIONAL**

Confidentiality of personal information of any person associated with Matamata Christian School (MCS) is fundamental.

**PURPOSE**

To ensure that MCS meets the requirements of the Privacy Act 1993 and its amendments.

**POLICY STATEMENT**

The Board of Trustees (BOT) has overall responsibility for the confidentiality of personal information held by MCS, but delegates responsibility to the Principal for the day to day management of all personal information and the privacy thereof, and to act as Privacy Officer.

**PRINCIPAL RESPONSIBILITIES**

The **Principal** will be the **Privacy Officer** whose role is to:

* Encourage compliance by MCS with the information privacy principles.
* Deal with requests made to MCS under the Privacy Act (see **Information Request Procedure** in **Appendix A**)
* Work with the Commissioner in relation to investigations conducted under the Act.
* Ensure compliance by the agency with the Privacy Act.
* Ensure all staff have received training on the management of information.
* Manage complaints and monitor any privacy issues (see **Privacy Complaint Procedure** in **Appendix A**)

**PROCEDURES**

1. In particular the **Principal** will:
2. Ensure that only personal information that is required to meet statutory requirements, administrative purposes, or to support the health and safety needs of individuals, is collected.
3. Obtain information directly from the person concerned, wherever possible, or from someone who is authorised to provide the information.
4. Ensure that forms (including **Enrolment Forms** and **Application Forms**) explain why the information is being collected, who will have access to it, and the purpose for which it will be used.
5. Ensure that only teachers or administration staff can access ASSEMBLY or child enrolment forms. Any computer with access to ASSEMBLY will have password access only. If the staff member using ASSEMBLY has to leave their computer for any period of time (especially where members of the public are situated) then the staff member will log out of the programme.
6. Store all personal information in a locked cabinet, ensuring employee information is accessible only by the Principal or relevant Administrator.
7. Store information for at least 7 years after the last contact, after which time it will be destroyed in a secure manner by secure document destruction.
8. Obtain written consent from the concerned party before sharing information, unless however the request is to support the safety of the child ie. from The Ministry for Vulnerable Children or the Police, then information will be shared.
9. Provide dual copies of the child’s school reports if the parents/guardians of the child do not live together, allowing both access to the child’s personal information, unless prohibited by court order.
10. Ensure that only accurate and up-to-date information is held on file. Parents/guardians and staff have the right to view and make changes to any information that is held about them or their child.
11. In particular the **Board of Trustees** will, where necessary to protect the privacy of an individual who is being discussed at the meeting, pass a resolution that the discussion be held “in committee”, and ensure relevant minutes to that part of the meeting are not publicly available.

**Appendix A**

|  |
| --- |
| **INFORMATION REQUEST PROCEDURE** |

|  |
| --- |
| **PRIVACY COMPLAINT PROCEDURE** |

|  |
| --- |
| **Privacy Officer** receives information request |

|  |
| --- |
| **Privacy Officer** receives privacy complaint |

|  |
| --- |
| Establish relevant IPP’s eg. 6 or 11  (see **Individual Privacy Principles** below) |

|  |
| --- |
| Determine nature of complaint – which IPP’s relate  (see **Individual Privacy Principles** below) |

|  |
| --- |
| Clarify supporting evidence |

|  |
| --- |
| Check identity of individual making request |

|  |
| --- |
| Identify what information is being requested and establish if that information is held |

|  |
| --- |
| Discuss with complainant and resolve |

|  |
| --- |
| If written consent is obtained provide information to individual within 21 days |

|  |
| --- |
| If consent is NOT obtained inform individual of grounds for refusal within 21 days |

|  |
| --- |
| Inform **BOT Chairperson** of complaint & resolution  or if complaint is unresolved formulate plan to address complaint with **BOT** and action. |

|  |
| --- |
| If individual is requesting access to another’s information (IPP11) seek written consent from the person concerned |

|  |
| --- |
| If individual is requesting access to their own information (IPP6) provide information |

|  |
| --- |
| If unresolved **Privacy Officer** may contact **Privacy Commissioner** or seek assistance from an agreed **Christian Dispute Resolution Service** |

|  |
| --- |
| As far as is practical, the process will be carried out in a timely manner.  Where there are conflicts of interest, the BOT shall nominate a representative to lead the process. |

|  |  |
| --- | --- |
| **INDIVIDUAL PRIVACY PRINCIPLES** | |
| 1. Purpose of collection of personal information 2. Source of personal information 3. Collection of information from subject 4. Manner of collection of personal information 5. Storage and security of personal information 6. Access to personal information | 1. Correction of personal information 2. Accuracy of personal information checked before use 3. Keep personal information no longer than necessary 4. Limits on use of personal information 5. Limits on disclosure of personal information 6. Unique identifiers |