Carmel Ministries International Data Protection Policy

Policy Statement

Carmel Ministries International(CMI) intends to fully comply with all requirements of the Data Protection Act 1998 ('Act') in so far as it affects CMI's activities. It also considers the provisions of the General Data Protection Regulation.

Scope of this policy

Carmel Ministries International (CMI) needs to comply with the Data Protection Act 1998 in relation to all personal data. To ensure this happens, it has developed this policy which sets out the obligations of staff in this respect.

The policy applies to all other services and ministries within Carmel Ministries International such as Carmel Christian School (CCS), Carmel Bible Institute (CBI), Carmel Children's Church, Youth Ministry etc.

This policy and the Data Protection Act apply to all personal data handled by CMI, both that held in paper files and data held electronically. So long as the processing of the data is carried out for CMI purposes, it also applies regardless of where data is held, (for example, it covers data held on the premises and on mobile devices such as on electronic notebooks or laptops) and regardless of who owns the PC/device on which it is stored.

This policy applies to all Trustees, employees, other staff, volunteers, School Governors, and individuals about whom CMI processes personal information, as well as other partners and companies with which the CMI undertakes it business. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

'Processing' data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

Data Controllers

CMI are 'Data Controllers' under the Data Protection Act 1998 and are registered with the Information Commissioner's Office on the following website:

https://ico.org.uk/for-organisations/register/

Review frequency: At least every two years (Registration is annual).

Legislation: The Data Protection Act 1998 (with consideration to the eight data protection principles appearing in Schedule 1):

http://www.legislation.gov.uk/ukpga/1998/29/contents

Carmel Ministries International Data Protection Policy

We at Carmel Ministries International are the Data Controller for the purposes of the Data Protection Act.

CMI is required under Data Protection legislation to comply with essential good practice in respect of the information collected here and to manage it securely. All records will be kept confidential. We will not pass on information to any third parties unless we have received permission to do so. The individuals who are the subject of the information or who have parental/ guardian responsibility are generally entitled to see the information and are encouraged to help keep the information up to date. This information will be used for educational, planning or managerial purposes and to keep parents and staff informed of school events and dates.

Carmel Christian School also have a duty to issue a Fair Processing (Privacy) Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Definitions

Personal data

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

We need to collect and use certain types of personal information about people with whom we deal in order to operate. These include current, past and prospective employees, pupils, suppliers, clients, and others with whom we communicate. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments.

This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998. We regard the lawful and correct treatment of personal information by the School as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The School wishes to ensure that it treats personal information lawfully, correctly and in compliance with the 1998 Act.

To this end we fully endorse the obligations of the Act and adhere to the Principles of Data Protection, as enumerated in the 1998 Act.

We collect information from members of the church, young people attending youth services, parents/carers and may receive information about students from their previous school. We hold this personal data and use it to:

- Provide appropriate pastoral care,
- Monitor and report on progress;
- Support teaching and learning;

- Assess how well the school is doing.

This information includes contact details, attendance information, characteristics such as ethnic group, gender, demographics, special educational needs and any relevant medical information.

We will not give information to anyone outside CMI without consent unless the law and our rules permit it.

We are required by law to pass some information to the Local Authority (LA), and the Department for Education (DfE).

If anyone would like to see a copy of the information we hold and share about them personally, then please contact the Data Protection Officer.

Individual Consent

In most cases, CMI can only process personal data with the consent of the individual whom the data concerns. If the information is sensitive personal data, explicit consent may be needed. However, it is a condition of student enrolment and of staff employment that they agree to CMI processing certain personal information as part of CMI's statutory obligations.

Sensitive personal data

CMI may process some information that is categorised as "sensitive personal data"; this includes information about an individual's racial or ethnic origin, gender, religion and beliefs, sexual orientation, physical or mental health, trade union membership and criminal convictions, charges or proceedings. This information may be required to comply with certain government or funding body regulations for example Ofsted, to ensure safety or to meet the requirements of CMI's policies and procedures.

Staff working in certain areas (eg CCS), or in certain roles (eg HR) will have regular access to sensitive personal data, others are likely to do so only rarely if at all. The majority of staff (including all line managers) will therefore handle personal data at least occasionally.

Confidential data

Data given in confidence or data agreed to be kept confidential, in other words a secret between two parties, and that is not in the public domain.

Some confidential data will also be personal data and/or sensitive personal data and therefore come within the terms of this policy. Staff working in certain functions and in senior management roles will handle confidential data regularly.

Legal framework

CMI needs to collect and keep certain types of information about the people with whom it deals. This includes information relating to its staff, students, members, volunteers and other individuals. It needs to process 'personal data' for a variety of reasons, such as to recruit and pay its staff, to record the academic progress of its students and to comply with statutory obligations (for example, health & safety requirements).

The Data Protection Act 1998 applies to all 'personal data' processed by CMI and to comply with the law, all personal data must be collected and used fairly, stored safely and not disclosed to any third party unlawfully.

Responsibilities of staff, volunteers and students

This policy is not part of the formal contract of employment, but it is a condition of all employment contracts that employees will follow the rules and policies created by CMI from time to time. Failure to follow the policy can result in disciplinary action being taken.

All partner agreements must include appropriate clauses relating to CMI's Data Protection Policy and approved procedures for recording, using and/or processing personal data.

All staff and students must:

1. Be mindful of the fact that individuals have the right to see their 'personal data' (and this may include for example information received from prospective students or staff written in connection with an application to CMI or any comments written about them in emails). They should not therefore record comments or other data about individuals which they would not be comfortable in the individual seeing, either in emails or elsewhere.
2. Immediately report the matter to their line manager and bring it to the Data Protection team's attention, if they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).
3. Immediately report the matter to their line manager and bring it to the Data Protection team's attention, if they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed (for example, if their laptop is stolen or their phone is lost and it has personal data stored on it),
4. Hold the contents of any personal data which comes into their possession securely.
5. Ensure that any personal data they provide to CMI (for example, their contact details) is accurate.
6. Notify CMI promptly of any changes to their personal data (for example, change of address or emergency contact details).
7. Only ever obtain or use personal data relating to third parties for approved work or study-related purposes.

Staff and students with access to 'personal data' must:

1. Ensure that they only ever process personal data in accordance with requirements of the Data Protection Act 1998 and in particular follow the 8 Principles it contains. The best way to ensure compliance is through familiarisation with this policy and the guidance we provide. Key points insofar as compliance is concerned include:

    - Fair processing – for example, ensure that the individual consents to their data being used and knows what it will be used for, and ensure that it is not subsequently used for something else
    - Data Security – ensure any personal data which is held is always kept and disposed of securely, (taking into account any cyber security considerations).
    - Non-disclosure – ensure personal data is not disclosed to any authorised third party.
2. Familiarise themselves with the guidance and other information published on our Data Protection site and follow it at all times.
3. If they are going to be working remotely or using a mobile device to store data (for example, a laptop, tablet or mobile phone), it is vital that they are familiar with our Remote Working & Use of Mobile Devices Guidance, and comply with it and with the CMI's IT Security Policy as special considerations apply.
4. Be mindful of the scope of Data Protection regulation. This includes that fact that 'personal data' is widely defined, (and so will cover for example comments made about an individual in an email to someone else), and the fact that it covers data held on remote devices (such as tablets and on mobile phones) regardless of who owns the actual device and where the device is stored.
5. Seek advice whenever a new or novel form of processing personal data is contemplated or if any data protection related concerns ever arise.

Personal Data in the public domain

Carmel Ministries International (CMI) holds certain information about staff and students in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available and may be disclosed to third parties without recourse to the data subject.

CMI's practice is to make the following items of data freely available unless individuals have objected:

- names of members of Senior Management
- staff work place email addresses and telephone numbers
- names of staff where appropriate
- any additional information relating to data subjects which they have agreed to be placed in the public domain and which may be in automated and/or manual form.

Similarly, as part of its regular business activities CMI may process personal information about third parties which is already in the public domain where such processing is carried out in accordance with the Data Protection Act principles set out below and is unlikely to cause any damage or distress to the data subject.

Data Protection Principles

Specifically, the Principles require that personal information:

- shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions as set out in the 1998 Act are met;
- shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- shall be accurate and, where necessary, kept up to date;
- shall not be kept for longer than is necessary for that purpose or those purposes;
- shall be processed in accordance with the rights of the data subject under the 1998 Act;
- shall be kept secure i.e. protected by an appropriate degree of security;

and that:

- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Our Commitment

CMI will, through appropriate management and application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act.
- take appropriate technical and organisational security measures to safeguard personal information;

and

- ensure that personal information is not transferred abroad without suitable safeguards.

Compliance

In addition, CMI will take steps to ensure that:

- there is an understanding that everyone is personally responsible for Data Protection within CMI
- everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- methods of handling personal information are regularly assessed and evaluated;

and

- it disseminates to employees, information on good practice in respect of handling, using, and storing personal information.

Data security

Keeping personal data properly secure is key in complying with the Data Protection Act. All staff are therefore responsible for ensuring that if they keep any personal data, it is kept securely and is not disclosed (either orally or in writing or accidentally) to any unauthorised third party.

Information Disclosure

CMI requires all staff, volunteers, students, contractors, partnership organisations and partner staff to be vigilant and exercise caution when asked to provide personal data held on another individual. In particular, they must ensure that personal information is not disclosed either orally or in writing to any unauthorised personnel, which includes family members, friends, government bodies and in certain circumstances the police, without the express prior consent of the relevant individual.

Please see the guidance on Disclosing Data for further information on this point.

Procedure for keeping personal data secure

This includes, as a minimum:

All staff, students, contractors, partnership organisations and partner staff must ensure that any personal information which they hold is kept securely and that they take appropriate security precautions by seeking to ensure the following:

- All staff (employed and voluntary) must take appropriate technical and organisational security measures to safeguard personal information.

- Source documents kept in a lockable cabinet or drawer or room;
- Computerised data is password protected;
- Data kept on discs or data storage devices are stored securely and encrypted;
- Ensure individual passwords are kept confidential and are not disclosed to other personnel enabling log-in under another individual's personal username and password;
- Logged on PCs are not left unattended where data is visible on screen to unauthorised personnel;
- Screensavers are used at all times;
- Paper-based records must never be left where unauthorised personnel can read or gain access to them.

- Personal information must be protected from unauthorised or accidental disclosure.
- Staff are responsible for ensuring that the personal information which they use during their role is appropriately secured and any concerns regarding its security are brought to the attention of The Data Protection Officer / Lead. This includes ensuring that personal information is removed from desks out of hours and sensitive personal information is locked in filing cabinets or desks when not in use.
- The Data Protection Officer / Lead is responsible for ensuring that personal information when in use is only accessible by those with a need and right to access it to perform their function or role.
- Staff must respect the privacy of the subject of the personal information they are handling by treating personal information about others as we would expect information about ourselves to be treated.
- Careful consideration must be given to the transmitting of Personal Data. Personal data must not normally be transmitted **externally** via email. **Although it is acceptable to transmit personal data internally, you should consider choosing another method if possible.**
- Personal information must be disposed of safely and securely.
- Documents and any storage media containing input to and output from systems (paper or electronic) detailing personal information must be held, transported and disposed of with due regard to its sensitivity.
- Where information is particularly sensitive it may be appropriate to ensure that the information is shredded on site.
- Publishing personal information on the Internet would make it available internationally therefore personal information must not be published on the internet, other than the names and work contact details of some employees and members if appropriate to their role.

When manual records are no longer required, they should be shredded or bagged and disposed of securely and the hard drives of redundant PCs should be wiped clean.

Off-site use of personal data presents a greater risk of loss, theft or damage and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. For these reasons staff and others should:

- only take personal data off-site when absolutely necessary and for the shortest possible time;
- take particular care when laptops or personal machines are used to process personal data at home or in locations outside of CMI, they are kept secure at all times.

Please see the section on data security and CMI's IT Security Policy for further information and rules on security.

Use of Images

An 'image' is personal data if the subject can be identified and therefore the Data Protection Act 1998 principles apply. Photographs, videos and webcams of *clearly identifiable people* must not be processed for any other purpose other than that it was originally collected for.

The school and children's church will get the permission for all use of photographic images and video footage by ensuring parents sign a consent form when a child is admitted to the school or children's church.

Images taken (including video) at an event attended by others, such as a sports event or assemblies are only to be used for personal viewing (or if taken by the school the purpose for which it is being collected) and the person in charge should address everyone to alert them to this and give them the opportunity to move away.

In the case of children, the purpose for which the images are to be used should be covered by a specific consent form, but if not a separate, signed parental consent form for each child will be obtained for that specific project.

Photographic/Video images used on a website will not include the child's first name in the accompanying text or photo caption. If a child is named in the text, a photograph will not be included unless specific parental consent has been given.

Photographs may be taken for security reasons to enable access to buildings for example and this is a legitimate business purpose for processing personal data.

Prohibited activities

Unacceptable use includes:

- unauthorised access of personal information
- unauthorised disclosure of personal information

- unauthorised use of personal information (e.g. not for reason given to access personal information)
- non adherence to CMI's information-sharing protocol
- unauthorised deletion

Employee or customer personal information must not be used for:

- any illegal purpose;
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the school into disrepute;
- any purpose which is not in accordance with the staff member's role or job description.
- using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for HR-related purposes for marketing purposes)
- disclosing personal data to a third person outside of CMI without the consent of the data subject.

This is not an exhaustive list. Cases where staff do not comply with this Policy or legislation will be dealt with under the Disciplinary Procedure and, depending on the circumstances; non-compliance may be deemed an act of gross misconduct.

Staff are required to notify an appropriate person, if they become aware, or suspect that personal information is being misused or handled inappropriately.

Rights of Individuals

Under the Act, an individual has the following rights:

1 To request access to information held about them, the purpose for which the information is being used and those to whom it is, has or can be disclosed to;

2 To prevent data processing that is likely to cause distress or damage;

3 To prevent data processing for direct marketing reasons;

4 To be informed about the reasons behind any automatic decision made;

5 To seek compensation if they suffer damage as a result of any breach of the Act by the Data Controller;

6 To take action to stop the use of, rectify, erase, or dispose of inaccurate information;

7 To ask the Information Commissioner to assess if any Personal Data processing has not been followed in accordance with the Act. Rights to access information

Any person who wishes to exercise this right should see the Subject Access Rights Page for details of how to do so.

Surveys- special considerations

Before commencing any survey which will involve obtaining or using personal data, the member of staff and their Line Manager must give proper consideration to this policy and the guidance contained on the our Data Protection section and how these will be properly complied with.

In particular, they will need to consider the type of personal data which may be collated, how consent is to be recorded, the extent to which such data may legitimately be required, how the data will be securely stored, (particularly if the data is what might be considered to be security-sensitive) and the duration for which it will be retained.

Personal data obtained or used for survey should be limited to the minimum amount of data which is reasonably required to achieve the desired objectives and wherever possible any such personal data should be made anonymous so that the data subjects cannot be identified.

Access to Personal Data

Subject to exemptions, the Act gives any individual who has personal data kept about them at CMI the right to request in writing a copy of the information held relating to the individual in electronic format and also in some manual filling systems. Any person who wants to exercise this right should in the first instance make a written request to CMI, using CMI's 'Subject Access Form'. CMI will make an administrative charge of £10 each time that a request is made.

After receipt of a written request, the fee and any information needed as proof of identity of the person making the request, CMI will ensure that the individual receives access within 30 calendar days, unless there is a valid reason for delay or an exemption is applicable. Subject Access requests will be supplied within 15 days for pupils.

The Act does not prevent an individual making a subject access request via a third party, including by a solicitor acting on behalf of a client. In these cases and prior to the disclosure of any personal information, CMI would need to be satisfied that the third party making the request is entitled to act on behalf of the individual and would require evidence of this entitlement.

Whilst the Act does not limit the number of subject access requests an individual can make to any organisation, CMI is not obliged to comply with an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

Submit a Subject Access Request

All Subject Access Requests must be made in writing to the Data Protection Officer. To ensure that your request is processed quickly, please:

- download our **Subject Access Request form**
- complete and print the form
- make a photocopy of suitable personal identification (driving licence or passport).

Send this information to:

Data Protection Officer

Carmel Ministries International

817A Bath Road

Brislington

Bristol

BS4 5NL

Direct Marketing (the communication by whatever means of any advertising or marketing material which is directed to individuals)

Under the Act an individual has the right to prevent his/her personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if CMI receives a notice then it must comply within a reasonable period. Any marketing campaign should be permission-based with a clear explanation of what an individual's details will be used for and a simple way should be included for an individual to opt out of marketing messages

Accuracy of Data

Staff , volunteers, members, parents and students are responsible for:

1 ensuring that any information they provide to CMI relating to their employment is accurate and up to date;

2 informing CMI of any information changes, eg. change of address; and

3 checking the information that CMI may send out from time to time giving details of information kept and processed about staff.

Students must also ensure that all data provided to CMI is accurate and up-to-date by either notifying the School/CBI Office with any changes to their address or personal details.

CMI cannot be held responsible for any errors unless the member of staff or student has informed CMI about them.

Retention and Disposal of Data

CMI is not permitted to keep personal information of either students or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements.

Personal and confidential information will be disposed of by means that protect the rights of those individuals ie. shredding, disposal of confidential waste, secure electronic deletion.

For further Information, not the Retention of Information Procedure.

Report a breach

If you suspect that a breach of the Data Protection Act has or may have occurred, you should immediately contact the Data Protection Officer.
You should provide as much information as possible, including:

- what information is involved, to whom it pertains and the number of individuals' data involved
- what happened to it - lost, stolen, or inadvertently disclosed
- how the breach may have happened?
- actions taken so far.

Data protection breaches include the accidental loss of data. This could involve a lost laptop or mobile phone with personal data stored on it or lost hard copies of files.

Even the loss or accidental disclosure of data relating to just one person can be of serious concern, particularly if it includes sensitive data such as health information, and should be reported immediately.

Any member of staff who realises that they have caused personal data to be lost or inadvertently disclosed must report the matter. Even if you have not been directly involved in the loss or disclosure, you are obliged to report the matter immediately

Complaints

CMI is dedicated to being compliant with the Act. Individuals, any member of staff or a student wishing to report concerns relating to the Act should, in the first instance, contact the following member of staff who as CMI's Data Protection Officer will aim to resolve any issue:

Data Protection Officer

The Data Protection Officer for CMI is Mona van Wyk.

17A Bath Road

Brislington

Bristol

BS4 5 NL

If the individual, member of staff or student feels the complaint has not been dealt with to their satisfaction, he/she can formally complain to the Overseer of Assets.

Implications of breaching this policy

It is a condition of employment in the case of staff and enrolment in the case of students that staff and students will abide by the policies and rules of CMI. Any breach of this policy will be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the CMI and/or the individual being held liable in law.

Conclusion

Compliance with the Data Protection Act 1998 is the responsibility of all members of CMI. Any questions about this policy or any queries concerning data protection matters should be raised with the Data Protection team at CMI.

Related Policies

1. Retention Guidelines
2. Information Audit
3. Photography and Filming
4. Good Practice for Managing E-mail
5. Information and Business Continuity
6. Pupil Records
7. School Data Breach Procedure
8. Safe Disposal of Records
9. Digital Continuity
10. Data Privacy Notice

Template documents:

1. Photograph Consent Form for Using Images of Children
2. Data Protection Act Subject Access Request Form
3. Information Asset Register
4. Notice for taking photographs/videos
5. Consent Form CMI
6. Consent Form1 CCS
7. Consent Form 2 CCS
8. Consent Form 1 Children's Church
9. Consent Form 2 Children's Church
10. Gift Aid Declaration Form
11. Information Management Survey Template
12. Photos will be taken Sign
13. School Photo Consent