# The Mount Camphill Community

# Data Protection Policy

| POLICY DETAILS | |
|---|---|
| Reference number | |
| Person responsible | Glen Farmer |
| Version History | Dec 2022<br>June 2020<br>June 2018<br>June 2016<br>Sept 2014 |
| Review date | June 2024 |
| Trustee submission date | June 2024 |
| Next review due | June 2026 |
| Associated documents/policies | Recruitment policy and procedures<br>Mental Capacity Act Policy<br>Staff Code of Conduct<br>Data Retention Policy<br>Information Security Policy<br>Safeguarding Policy |

| IMPACT ASSESSMENT | | |
|---|---|---|
| Name | Comments | Date |
| | | |

| AUTHORISATION | |
|---|---|
| Approved by (Chair of trustees) | Date |
| Peter Bateson | |

# The Mount Camphill Community

# Data Protection Policy

## Contents

# The Mount Camphill Community

# Data Protection Policy

## 1. Aims

The Mount Camphill Community aims to ensure that all personal data collected about employed colleagues and co-workers, students, Cohousers, parents, Trustees, volunteers, visitors and other individuals is collected, stored and processed in accordance with the applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

## 2. Scopes and objectives of this Data Protection Policy

This policy is the binding framework for the compliant handling and processing of personal data by the Mount Camphill Community. The implementation of this policy aims to protect the fundamental rights and freedoms of data subjects and to ensure an appropriate level of data protection against the risks of processing personal data. The main objective of the policy is to bring all data processing activities in line with the applicable data protection legislation (in particular, the UK General Data Protection Regulation).

The provisions of this policy apply to all employees, co-workers, managers and anyone else who may have access to personal data as part of their role at the Mount Camphill Community. The policy is made available to every individual at the start of their employment and can be accessed at any time through the organisation's internal system.

This policy applies to all operations and activities in which the personal data of individuals is processed. It is irrelevant whether the processing of personal data is carried out electronically or in paper form.

The provisions of this policy supplement, but do not replace, the applicable data protection legislation. In the event of a conflict or divergence between the applicable data protection legislation and the provisions of this policy, the applicable data protection legislation shall prevail.

This policy may only be amended with the approval of the Data Protection Officer. The organisation, or any affiliated entity, may not implement any diverging policies.

Management is responsible for determining when this policy comes into force.

## 2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data |

| | |
|---|---|
| | • Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| **Criminal offence data** | Personal data relating to criminal convictions and offences or related security measures, including:<br>• Criminal activity<br>• Allegations (including unproven allegations)<br>• Investigations<br>• Proceedings<br>• Information relating to the absence of convictions<br>• Information related to security measures, such as penalties or conditions imposed as part of the criminal justice process |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br>Processing can be automated or manual. |

| | |
|---|---|
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

## 4. The data controller

The Mount Camphill Community determines the means and purposes of processing personal data relating to parents, students, Cohousers, employed colleagues and co-workers, trustees, visitors and others, and therefore is a data controller.

The Mount Camphill Community is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

This policy applies to **all employed colleagues, volunteers and co-workers** of The Mount Camphill Community, and to **external organisations** or **individuals** working on our behalf. Employed colleagues and co-workers who do not comply with this policy may face disciplinary action.

### 5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that The Mount Camphill Community complies with all relevant data protection obligations.

### 5.2 Data protection officer

The Data Protection Officer shall monitor compliance with the applicable data protection legislation and this policy. The Data Protection Officer advises and informs the management of their obligations under data protection law. In addition, the Data Protection Officer acts as a contact point for data subjects and supervisory authorities on issues relating to the processing of personal data.

The Data Protection Officer shall not receive any instructions regarding the exercise of these tasks and reports directly to the highest level of management.

The Moun Camphill Community has appointed the following external Data Protection Officer:

DataCo International UK Limited

Suite 1, 7th Floor, 50 Broadway, London, England, SW1H 0BL

privacy@dataguard.co.uk

www.dataguard.co.uk

Employees may contact the Data Protection Officer at any time. In particular, the Data Protection Officer should be involved as early as possible in the following issues:

- Data subject requests or enquiries
- Enquiries from the supervisory authorities
- Data breaches (incidents affecting personal data)
- Enquires on data protection documentation
- Corporate strategies related to data protection
- Data protection compliance of offered products and services as well as the use of tools and software.

Our external DPO is DataGuard and is contactable via our internal data protection coordinator glen.farmer@mountcamphill.org or by phone internal extension 224,external 01892 786153 .

### 5.3 The Management Group

The Management Group acts as the representative of the data controller on a day-to-day basis.

### 5.4 All employed colleagues and co-workers

Employed colleagues and co-workers are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing The Mount Camphill Community of any changes to their personal data, such as a change of address
- Contacting the internal data protection coordinator and DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

## 6. Data protection principles

The UK GDPR is based on data protection principles that The Mount Camphill Community must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

In addition, the principles of data protection must be integrated into Mount Camphill Community's internal software applications, data processing activities and services (data protection by design/privacy by default). When selecting data processing systems, the highest data protection settings and configurations must be set by default.

This policy sets out how The Mount Camphill Community aims to comply with these principles.

# 7. Collecting personal data

## 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that The Mount Camphill Community can **fulfil a contract** with the individual, or the individual has asked The Mount Camphill Community to take specific steps before entering into a contract
- The data needs to be processed so that The Mount Camphill Community can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that The Mount Camphill Community, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of The Mount Camphill Community or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student or Cohouser) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

For criminal offence data, we will also meet a specific condition for processing in Schedule 1 of the Data Protection Act 2018.

These conditions must be met before the personal data is processed.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

## 7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we may only do so in compliance with applicable Data Protection law. Personal data may not be used for a new purpose unless it is compatible with the original purpose, we have the consent of the individual concerned or there is a clear obligation or function set out in law..

Employed colleagues and co-workers must only process personal data where it is necessary to allow them to do their jobs.

When employed colleagues and co-workers no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with The Mount Camphill Community's Data Retention Policy and it's Information Security Policy.

## 8. Data processing by third parties

Where personal data is processed on behalf of the data controller, a data processing agreement must be concluded with the data processor. This agreement must also comply with the requirements of Article 28 of the UK GDPR. In the relationship between a data controller and a data processor, the processor must act only under the instructions of the controller.

Irrespective of the instructed processing, the data controller must always ensure that personal data is processed in accordance with the data protection principles. When selecting the data processor, the data controller must ensure that the data processor is professionally able and has appropriate technical and organisational measures in place.

If the data processor provides its services in a third country (country outside the UK) or if the data processor uses the services of another data processor located in a third country, the data controller must ensure that the data transfer takes place on the basis of an adequacy decision or an appropriate transfer mechanism as per Chapter V of the UK GDPR. Transfers of personal data to third countries must always be discussed in advance with the Data Protection Officer.

## 9. Sharing personal data

Sometimes, we need to share personal data with third parties. For example, we are required to share some personal data with Local Authorities when admitting a student we need to submit a needs assessment in order to obtain funding.

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student, Cohouser or parent/carer that puts the safety of other members of the Mount Camphill Community at risk
- We need to liaise with other agencies (for example Healthcare professionals, Local Authorities, Alternative placement providers, Regulatory bodies and Awarding organisations– we will seek consent when necessary before doing this).
- We need to provide relevant information to companies who are placing students on work experience
- Our suppliers or contractors need data to enable us to provide services to our employed colleagues and co-workers, students and Cohousers – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud

- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any members of The Mount Camphill Community.

Personal data should only be shared with third parties when we have the power to share and an appropriate lawful basis (and any other applicable condition in respect to special category or criminal offence data) has been identified. All decisions relating to information sharing should be clearly documented so we can demonstrate our compliance. Personal data should only be shared if doing so is fair, necessary and proportionate. Consideration should also be given to what safeguards need to be put in place to share the personal data securely.

Where we need to share data with an organisation that is based outside the UK, we will only do so in compliance with Chapter V of the UK GDPR.

Personal data should be shared in accordance with applicable Data Protection laws, including the ICO's data sharing code where applicable.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that The Mount Camphill Community holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests can be made either in writing or verbally, including but not limited to: email, letter or on social media. A request is valid if it is clear the individual is asking for their own personal data. An individual does not need to use specific words, refer to legislation or direct the request to a specific contact.

If employed colleagues and co-workers receive a subject access request they must immediately forward it to the internal data protection coordinator who will liaise with the DPO.

### 9.2 Children and subject access requests (Students aged under 18)

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at The Mount Camphill Community may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

The Mental Capacity Act 2005 (MCA) works with the principle of assuming capacity. The Mount Camphill Community would support a student in various ways to understand the issue of a subject access request. This can happen verbally or pictorially working closely with the expectations of the MCA. If The Mount Camphill Community concludes that a student may lack the capacity to understand the issue and consequences of a subject access request a mental capacity assessment would be undertaken and the decision for a subject access request would become a best interest decision if it is shown that the student lacks capacity for this particular issue.

For more guidance on the rights of children under the UK GDPR, please refer to the ICO's guidance.

### 9.3 Responding to subject access requests

When responding to requests, we:

- Need to be satisfied that we know the identity of the requester (or the person the request is made on behalf of) and the data we holds relates to the individual in question. We may ask for enough information to judge whether the requester is the person the data is about. It is important we are reasonable and proportionate about how we confirm this information. This will often depend on the circumstances of how the request was received. Formal identification documents should only be requested if they are necessary. Please reach out to the Data Protection Officer if you need any support with this.
- Will respond without delay and within 1 month of receipt of the request or receipt of any information required to confirm the requester's identity unless an exception applies (
- Will provide the information free of charge
- May extend the time to respond by a further 2 months if the request is complex or we have received a number of requests from the individual. If we decide it is necessary to extend the time limit by 2 months, we must let the individual know within one month or receiving their request and explain why.
- Consider where information pertaining to the request may be kept and search all records as required (e.g. this may include hard copy records, emails, files, external hard-drives, CCTV footage, etc).
- Check whether any information needs to be redacted (e.g. because it does not relate to the individual) before we consider giving a requester information.
- Consider the impact of releasing personal data about other people and consult the external Data Protect Officer for guidance on whether it would be appropriate to withhold personal data relating to third parties.
- Securely send the reply, including the required privacy information.
- Keep records of the information sent for accountability purposes.

Schedules 2 and 3 of the Data Protection Act 2018 set out the exemptions to complying with data subject rights requests. Please speak to the Data Protection Officer for guidance on the circumstances it would be appropriate to rely on an exemption. Examples of when we will not disclose information include if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

It is the view of the ICO that a subject access request relates to the data held at the time the request was received. Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

### 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time where our lawful basis for processing the data has been given by us as "consent"
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Object to the use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK GDPR
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals may submit any request to exercise these rights to the internal data protection coordinator who will liaise with the DPO. If employed colleagues and co-workers receive such a request, they must immediately forward it to the internal data protection coordinator who will in turn liaise with the DPO.

## 10. Parental requests to see the educational record

As standard we will send parents/carers, or those with parental responsibility, copies of the students' study plans and programmes, reports and EHC Plans prior to all reviews. Further requests for information will be dealt with on an individual basis and we will respond to these requests within one calendar month of receiving them.

## 11. Photographs and videos

As part of The Mount Camphill Community activities, we may take photographs and record images of individuals within The Mount Camphill Community.

We will obtain written consent from parents/carers for students aged under 18, and from individuals over 18, for photographs and videos to be taken of students or Cohousers for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the individual how the photograph and/or video will be used.

The Mental Capacity Act 2005 (MCA) works with the principle of assuming capacity. The Mount Camphill Community would support a student/ co houser in various ways to understand the issue of a photograph and records consent. This can happen verbally or pictorially working closely with the expectations of the MCA. If The Mount Camphill Community concludes that a student/ co houser may lack the capacity to understand the issue and consequences of a photography and records consent a mental capacity assessment would be undertaken and the decision for a photography and records consent would become a best interest decision if it is shown that the student/ co houser lacks capacity for this particular decision.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

See appendix 2 for more information on our use of photographs and videos.

Employed colleagues and co-workers should also see the staff code of conduct and the Information Security policies.

## 12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where The Mount Camphill Community's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training employed colleagues, co-workers, volunteers, trustees and individuals working on our behalf on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance (see section 16: Training)
- Keeping a record of attendance at all training sessions
- Conducting quarterly reviews and audits to test our privacy measures and make sure we are compliant as well as ongoing spot checks on Information Security basics such as locking computer screens and collecting prints from the printer.
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of The Mount Camphill Community and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, in workshops, on tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, employed colleagues and co-workers must first confirm the reason with their line manager and gain agreement to do so and then ensure the data is kept safe at all times.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Employed colleagues and co-workers and students/ co housers are reminded to change their passwords at regular intervals
- Employed colleagues and co-workers or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Information security policy and the staff code of conduct
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## 14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on The Mount Camphill Community's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

For more information, please refer to the Data Retention and Deletion Policy and Schedule.

## 15. Personal data breaches

The Mount Camphill Community will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in The Mount Camphill Community context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data about students, Cohousers or employed colleagues and co-workers
- The loss of paperwork containing personal data

## 16. Training

All employed colleagues, co-workers, volunteers, trustees and individuals working on our behalf are provided with data protection training as part of their induction process before processing personal data and within one month of their start-date.

We will provide refresher data protection training every year as part of continuing professional development, or more frequently where changes to legislation, guidance or The Mount Camphill Community's processes make it necessary.

We will keep a record of attendance at all training sessions on our Databridge system.

## 17. Monitoring arrangements

The internal data protection coordinator and DPO are responsible for monitoring and reviewing this policy.

This policy was first written when the Data Protection Bill received royal assent and became law (as the Data Protection Act 2018). The policy will policy will be reviewed **every 2 years** (or in the event of a significant change in legislation if earlier) and shared with the Board of Trustees.

## 18. Links with other policies

This data protection policy is linked to our:

- Mental Capacity Act Policy
- Safeguarding Policy
- Staff Code of Conduct
- Recruitment policy and procedures
- Mental Capacity Act Policy
- Staff Code of Conduct
- Data Retention and Deletion Policy
- Information Security Policy
- Safeguarding Policy

## Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the employed colleagues and co-workers member or data processor must immediately notify the DPO. This is done by completing the Data Breach report form (see attached) with the support of the data protection coordinator who will then send the completed form to the external DPO.
- The internal data protection coordinator and DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will provide a risk assessment to the internal data protection coordinator who will then alert the Co-ordinator for Education and the chair of the Board of Trustees
- The Mount Camphill Community with the support and guidance of the DPO, will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant employed colleagues and co-workers members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO and The Mount Camphill Community will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will assess whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, The Mount Camphill Community with the support of the DPO, must notify the ICO.
- The Mount Camphill Community will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on The Mount Camphill Community's computer system.
- Where the ICO must be notified, The Mount Camphill Community with the guidance and support of the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, this report will set out:
    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, The Mount Camphill Community with the guidance and support of the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when The Mount Camphill expects to have further information. The Mount Camphill Community with the guidance and support of the DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Mount Camphill Community will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Mount Camphill Community will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Mount Camphill Community will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be on The Mount Camphill Community's computer system.

  The DPO, the internal data protection coordinator, the Coordinator for Education and the Coordinator for Care will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

### Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

***For example: Sensitive information being disclosed via email (including safeguarding records)***

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of employed colleagues and co-workers who receive personal data sent in error must alert the sender and the internal data protection coordinator and DPO as soon as they become aware of the error*

- *If the sender is unavailable or cannot recall the email for any reason, the internal data protection coordinator will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the internal data protection coordinator will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The internal data protection coordinator will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The internal data protection coordinator will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

## Appendix 2 - The use of photographic and video images at The Mount

Photographs and videos of students and Cohousers and their work will be routinely taken throughout their time with us to support their record of progress at The Mount Camphill Community.

Where consent has been clearly and explicitly granted to use photographic and video images for other purposes these will normally be limited to publication as follows

1. Within The Mount Camphill Community on notice boards and in Mount magazines, brochures, newsletters, etc.
2. Outside of The Mount Camphill Community by external agencies such as newspapers, campaigns
3. Online on The Mount Camphill Community website, YouTube channel or social media pages
4. Individuals will not be named on any external publications without specific consent being given on each occasion this arises.