Data Protection Policy

Contents

Mary's is registered, as Data Controller, with the Information Commissioner's Office (ICO) and has submitted to the ICO the type of information it collects, holds and uses. These details are available on the ICO's website. Mary's has a duty to issue Privacy Notices to all of its data subjects or their legal guardian (if under 12 year of age) summarising the information held on them, why it is held and the other parties to whom it may be passed on.

Mary's is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

This policy sets out how we protect personal data and ensure that our staff and volunteers understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the CEO be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

We may use personal data for personnel, administrative, financial, safeguarding and other regulatory, payroll and business development purposes.

1 Definitions

Business purposes include the following:

- Compliance with our legal, regulatory and governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering ICT devices, use of email and the internet)
- Operational reasons, such as recording beneficiary attendance, transactions, training and quality control, ensuring the confidentiality of sensitive information, security and safeguarding vetting, identity checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data we gather may include individuals' name, address, *phone number, email address, educational backgrounds, social and financial backgrounds, pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, job application forms and CVs.*

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings — any use of special categories of personal data should be strictly controlled in accordance with this policy.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Supervisory authority

This is the national body responsible for data protection. The supervisory authority for Mary's is the Information Commissioner's Office.

2 Scope

This policy applies to all staff and volunteers, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3 Who is responsible for this policy?

The board of trustees are responsible for approving and reviewing this policy. The Data Protection Lead, Aston Wood (CEO), has overall responsibility for the day-to-day implementation of this policy. You should contact the CEO for further information about this policy if necessary.

Contact details: aston.wood@marys.org.uk. Tel: 020 7354 1387

4 The principles

Mary's shall comply with the principles of data protection (the Principles) contained in the UK General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

See: A guide to the data protection principles | ICO

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

7. Accountability and transparency

We must ensure accountability and transparency in our use of personal data. We must show how we comply with each Principle.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implementing all appropriate and reasonable technical and organisational measures
- Maintaining up-to-date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implementing measures to ensure privacy by design and default, including:
    - Data minimisation (collect and process only the necessary minimum amount of personal data needed to achieve the lawful processing purpose).
    - Pseudonymisation (replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms in such a way that the data can no longer be attributed to a specific data subject without the use of additional information).
    - Transparency (actively bring to the data subjects' attention the applicable privacy notices, changes to them or reminders to look at them again and again so data subjects remain fully aware of the controller's activities in relation to their personal data).
    - Allowing individuals to monitor processing (facilitating data subject access requests).
    - Creating and improving security and enhanced privacy procedures on an ongoing basis.

5 Our procedures

5.1 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless we have a clear lawful bases to do so.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed and erased.

5.2 Controlling vs. processing data

Mary's is classified as a data controller and processor. We must maintain our appropriate registration with the Information Commissioner's Office in order to continue lawfully controlling and processing data.

Typically Mary's will be acting as Data Controller but in the cases where Mary's is acting as data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of

processing outside the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Cooperate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If there is any doubt about how we handle data, contact the Data Protection Lead for clarification.

5.3 Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the Data Protection Lead. It is the data processor's responsibility to check the lawful basis for any data they are working with and ensure their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

- Consent - We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- Contract - The processing is necessary to fulfil or prepare a contract for the individual.
- Legal obligation - We have a legal obligation to process the data (excluding a contract).
- Vital interests - Processing the data is necessary to protect a person's life or in a medical situation.
- Public function - Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- Legitimate interest - The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

5.4 Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonable achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Data processors should use the Lawful Basis for Data Processing Assessment tool (Lawful basis interactive guidance tool | ICO) to help identify the correct lawful bases for processing.

You should also consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?

- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the Data Protection Lead.

6 Special categories of personal data

6.1 What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

7 Responsibilities

7.1 Youth Managers responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data and obtain the approval of the Data Protection Lead
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways according to agreed protocols
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Drafting data protection statements attached to emails and publicity
- Coordinating with the Data Protection Lead to ensure all marketing initiatives adhere to data protection laws and Mary's Data Protection Policy
- Drafting Privacy Notices and ensuring that these are issued as appropriate

7.2 Individual staff member and volunteer responsibilities

- Fully understand their data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay
- Issuing Privacy Notices to individuals as appropriate

7.3 Responsibilities of the Data Protection Lead

- Keeping the board updated about data protection responsibilities, risks and issues Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Ensure all systems, services, software and equipment meet acceptable security standards
- Ensure the checking and scanning of security hardware and software is carried out regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

- Keeping an up to date record of all datasets held by or processed by Mary's including any constraints on how long the data should be kept

7.4 Accuracy and relevance

Mary's will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the relevant service manager or CEO.

8 Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Data Protection Lead will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

8.1 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff and volunteers to use a password manager to create and store their passwords.
- Data stored on removable memory (such as disks or memory sticks) must be encrypted or password protected and locked away securely when they are not being used
- The Data Protection Lead must approve any cloud used to store personal data Servers containing personal data must be kept in a secure location
- Data should be regularly backed up
- Personal Data should not be saved/ downloaded directly to mobile devices such as laptops, tablets or smartphones unless it is necessary for off-site work (e.g. for outreach). In such circumstances, devices must be encrypted and password protected to prevent data breach in the event of loss or theft.
- All servers containing sensitive data must be approved and protected by security software All reasonably possible technical measures must be put in place to keep data secure

8.2 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

8.3 Destruction of data

When information reaches the expiry date for retention, ALL copies of that information must be permanently destroyed. Where information is held in more than one media the information must be removed from all record systems, for example, paper copies – shredded; electronic copies – completely destroyed from any memory source or other media.

All documents, including electronic documents, that are no longer relevant to the organisation's business, should be destroyed every thirty (30) days. Drafts of documents that have been finalised should not be retained.

Mary's should follow these guidelines for destruction of data and documents:

- do not deposit paper documents containing personal data or confidential information in the general waste bin. This could result in the unauthorised disclosure of such information to third parties and render Mary's liable to prosecution or other enforcement acts under the Data Protection Act. Such documents should be destroyed on-site, using shredders.
- Deletion: the Information Commissioner has advised that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent to deletion. If data is no longer relevant it should be deleted after thirty (30) days and if data is relevant it should be backed up.
- Recycling: wherever practicable, disposal should further recycling, in-line with Mary's commitment to sustainable development and promoting an alternative waste disposal strategy.

Disposal of significant documents should be documented by the relevant member of staff by keeping a record of the document disposed of, the date and method of disposal, and who authorised disposal. The documenting of disposal of personnel records will be particularly important for GDPR.

8.4 Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the CEO.

9 Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

Enabling individuals to access their personal data and supplementary information Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

This must be done without delay, and no later than one month. This can be extended to two months with permission from the Data Protection Lead.

4. Right to erasure

We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

We must provide individuals with their data so that they can reuse it for their own purposes or across different services.

We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

We must respect the right of an individual to object to direct marketing, including profiling.

We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision-making and profiling

We must respect the rights of individuals in relation to automated decision making and profiling.

Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

10 Privacy notices

10.1 Supplying a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

10.2 What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the Data Protection Lead
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place if applicable
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)
- The right of data subjects to request access to the data held on them and the procedure for processing such requests

11 Subject Access Requests

11.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

11.2 How we deal with subject access requests

We must provide an individual with a copy of the information they request, free of charge. All data subject access requests must be notified to the Data Protection Lead, who will oversee the response to the request. This must occur without delay. Response to the data subject must be sent , and within one month of the receipt / confirmation of the requestor's identity. We endeavour to provide

data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. The Data Protection Lead will decide if it is necessary to extend the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual to specify the information they are requesting. These decisions are to be made by the Data Protection Lead.

Once a subject access request has been made, the data requested must not change or be amended. Doing so is a criminal offence.

11.3 Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a Comma Separated Values (CSV) file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the CEO first.

12 Right to erasure

12.1 What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

12.2 How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

12.3 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

12.4 The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision-making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

13 Third parties

13.1 Using third-party controllers and processors

As a data controller, we must have written contracts in place with any third party data controllers and data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

13.2 Contracts

Our contracts with data processors must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

As a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

14 Criminal offence data

14.1 Criminal record checks (Disclosure & Barring Scheme checks)

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. The authorised role holders permitted to carry out these checks are:

- Youth Work Development Manager
- CEO

15 Audits, monitoring and training

15.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Regular data audits must be conducted as required by the CEO or Board of Trustees.

15.2 Monitoring

The Board of Trustees have overall responsibility for this policy. Mary's will keep this policy under review and amend or change it as required. You must notify the Data Protection Lead of any breaches of this policy. Staff and Volunteers must comply with this policy fully and at all times.

15.3 Training

Staff and Volunteers will receive adequate training on provisions of data protection law specific for their role. Staff and Volunteers must complete all training as requested. If Staff or Volunteer roles or responsibilities change, they are responsible for requesting new data protection training relevant to the new role or responsibilities.

If Staff or Volunteers require additional training on data protection matters, they should contact their line manager or the Data Protection Lead.

16 Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. Mary's has a legal obligation to report any data breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Data Protection Incident/Breach Log to report any data protection policy-related concerns. Data Protection Incident Log

16.1 Failure to comply

We take compliance with this policy very seriously. Failure to comply puts individuals, staff, volunteers and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any concerns or questions about this policy, do not hesitate to Contact the CEO.

17 Changes, Reviews and Approvals for this Policy

Date	Changes, Reviews and Approvals	Who By
21/07/2023	• Updated contact names • Formatting and readability changes.	Aston Wood
26/07/2023	Approval	Trustees