# Data Protection Policy

PUBLISHED
3 October 2019

# The Wesley Trust Data Protection Policy

| Reviewed By | Approved By | Date of Approval | Version Approved | Next Review Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Signed by chair of the Board of Trustees**……..

## Contents

## 1. Introduction

The Wesley Trust Data Protection Policy (the "Policy") sets out the principles for handling data responsibly and securely within the Wesley Trust ("the Trust") and its schools. This Policy is also related to data concerning natural persons about whom we hold data and is designed to fulfil the requirements of the General Data Protection Regulation ("GDPR") that come into force in May 2018 and the Data Protection Act 2018 ("DPA").

Schools are obliged by law to fulfil the requirements of the GDPR and the DPA and ensure that procedures are in place to satisfactorily assure that all areas of this policy are operating in practice.

In addition to this, the Trust is committed to ensuring that we have a safe data environment that respects the rights of all people that are affected by the scope of the GDPR, the DPA and beyond. Constant improvements in a changing data environment will be strived for, and systems and individuals falling below the standards expected will be challenged.

## 2. Key policy principles

- The Trust recognises that each of its schools is a public authority, as defined by the GDPR and must take accountability for this Policy in this context. As such we recognise that we are accountable for the data we control and have a responsibility to ensure those that process our data do so in line with the GDPR requirements.

- The Trust is serious about maintaining the highest standards of data management, ensuring that all people that are our data subjects are treated with respect and their rights are understood and held in high regard.

- The Trust will monitor its data environment and ensure that all data that we control or process is audited regularly and, if appropriate, assessment made as to the impact of data processing on our data subjects.

- Due regard will be given to the design of our systems so as to ensure that security of people's data is given high priority and that we will only hold data that is needed to lawfully and legitimately fulfil our organisation's operation. People within our organisation will only be given access to data that they need to carry out their roles and responsibilities at the school.

- We will uphold the rights of individuals to make legitimate requests for data, in a variety of categories as defined by the regulations and will respond to these requests reasonably and as laid out by the regulations.

- We will not hold data for longer than is reasonably needed and will dispose of time expired data in a suitable way given the level of sensitivity of the data.

- The Trust and its schools will ensure that the organisation has the necessary skill and support to respond to data requests, by having a suitably trained Data Protection Officer who will co-ordinate policy and procedures, respond to such requests and report to the board on progress against the requirements of the GDPR.

- Should any data breaches occur then these issues will be dealt with promptly and efficiently, as required by the Regulation and the DPA. The Trust will liaise with the Information Commissioner's Office, through the Data Protection Officer, and other agencies as directed in order to remedy these breaches and to learn lessons from any such breaches.

- The Trust will communicate with people that are classified as our data subjects (people who we hold data about) and will inform them of the type of data we hold about them via privacy notices and what the lawful reason for holding this personal data is, and for how long we will hold the data. This will ensure that our processes are transparent and that all people included in our data recording activities are treated fairly.

- The Trust will give training to all staff and other key stakeholders on data management with regard to the scope of the GDPR in order to ensure better data security and to specific staff on the management of data where that is appropriate to their role.

- Should the standards our school expects not be adhered to, accidentally or deliberately, then appropriate investigation will be conducted, recommendations made and remedial action taken, potentially including disciplinary action.

## 3. Our data

It is the responsibility of the Trust to ensure that we have a clear understanding of any data that we hold with regards to our data subjects (as defined by the GDPR).

This data will be understood at a granular level and the reason for holding this data must be understood. Furthermore, a lawful reason for holding this data must be established and documented in order to ensure that our data subjects are protected from inappropriate use of their personal data and to minimise the risk of identity fraud.

A data audit will be conducted to establish what data is being held and whether or not the data held complies with the requirements of the GDPR. This audit will be a detailed exercise and will establish a number of factors including:

A. all characteristics that are held with relation to the data subject
B. whether special category data is held
C. what the lawful reason for holding the data is
D. what system the data is held on
E. who is responsible for managing that data system
F. how long the data will be held for

Once the initial data audit is conducted further work will be done to ensure that all aspects of this policy are complied with, or that an action plan is in place to close gaps. A further audit will be conducted annually, with the aim of bringing the records of what data is held up to date, ensuring accuracy of those records and to ensure that new data systems have been included and their impact assessed and that data due for destruction has been destroyed securely.

## 4. Compliance with the Regulation and the DPA and managing information responsibly

As the data controller for information the schools of the Trust have a number of responsibilities with regard to ensuring that they comply with the requirements of the Regulation and the DPA.

We will ensure that these responsibilities are upheld by complying with the Regulation and the DPA and more specifically putting the following processes in place.

- Undertaking a data audit on an annual basis (as above) in order to ensure that we understand the data that we hold at all of the schools and have a record of our processing activities. Each school will be required to conduct a data audit annually.

- Reviewing the design of our data to ensure that we are minimising the risk of data breaches and that unnecessary data is not held in our systems

- Communicating with data subjects with reference to the data that we hold and why we hold it. This will be done through the issue of privacy notices, and in the case of our students will be delivered via their parents (for all children falling below the age of responsibility as defined by the GDPR and/or the DPA and the Information Commissioner's Office).

- Putting a process in place for managing all data requests received from our data subjects and others parties that may request information from our organisation. This process will ensure that all the rights of the individual as laid out in the Regulation and/or the DPA are respected and that timescales are adhered to.

- The Trust will appoint a Data Protection Officer who will be responsible for co-ordinating and implementing the policy of the Trust. They will ensure compliance across all the schools, report to the Board of Trustees on progress against the requirements of the policy and be the published contact point for requests for information.

- The Trust will put in place appropriate safeguards with its data processors in order to ensure that the requirements of the Regulation and/or the DPA are being complied with. This will include ensuring appropriate safeguards where data processing activity takes place outside the EC/EEA.

- A documented process will be put in place in order to ensure that data breaches and decisions made about communication with the Information Commissioner's Office and the data subjects of any such breach are recorded.

- Data retention periods for each element of data identified in the data audit process will be established and as part of the annual audit appropriate destruction /deletion of this data will be undertaken.

- The way in which data is used by data users in our organisation will be explained clearly and each user of data will be asked to record their understanding of their responsibilities. An acceptable use statement will be prepared for different information users so that it is clear to them how to use data in an acceptable way as a part of our school community.

- We will provide guidance, best practice and requirements for ensuring that online safety is promoted and monitored in our schoosl. This will be done in the best interests of the whole school community and will be reviewed regularly in order to ensure that the impact of developing technologies is taken into consideration.

## 5. Training and awareness

The training of staff and other users of data at our school will be given a high priority, to minimise the risk of inappropriate use of data, to minimise the risk of data breaches and promote the best practice in deliver the objectives of the school whilst respecting the rights of our data subjects.

Training will be given on a regular basis and will include different messages for different staff and users of data. Staff or other users of data that handle specific or special category data will be given further training as necessary to ensure that they are fully aware of the impact that they might have if data is not handled appropriately.

We will also promote awareness amongst the whole community of data users and data subjects alike to ensure that there is an awareness of the need for balancing the needs of the school in controlling and processing personal data with the rights of individuals in protecting their own data.

## 6. Review

Our data environment is extremely dynamic meaning that review of our approach to information systems must remain under review and keep up to date with recent developments. This will mean that this policy will be updated biennially and the schedules that inform the procedures that are in place for specific elements of our policy will be updated to reflect best practice and changing regulations. This will be done biennially as a minimum.

## 7. Schedules (to be added by each school)

All schools within the Trust will be responsible for maintaining and reviewing the schedules below as part of their commitment to data protection. The Trust will work with schools to ensure that this data is audited on a regular basis and that each school has a suitably qualified data protection officer in place to assist staff and governors on deploying the policy.

Acceptable use of ICT documents for data users

Data audit template and record of processing activity

Data impact Assessment

Privacy notices

Information request procedure

Data Breach Procedure

Data retention periods

Data self assessment / audit

Detailed DPO job description

Online safety guidance

Data user and stakeholder responsibilities