Overarching Data Protection Policy

Malvern College & The Downs Malvern

April 2023

1 Purpose

1.1 This document outlines the framework that the Schools have in place to help ensure compliance with data protection law, including the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**).

1.2 Any references to staff include all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, peripatetic staff, and volunteers.

2 Roles, Responsibilities and Governance

2.1 The governors have appointed Steve Cragg as Data Compliance Officer (henceforth: DCO). The DCO is responsible for managing the School's compliance with data protection law. The governors have ensured that the DCO has sufficient time and resources to fulfil their tasks.

2.2 The DCO regularly reports to the Malvern Executive Team and to the Governors' Audit Committee who are responsible for the Schools' data protection compliance. Data protection is a standing item on the agenda at governors' meetings.

2.3 The Audit Committee of governors has specific responsibility for data protection.

2.4 All staff have a role to play in our data protection compliance. Staff are encouraged to ask questions and raise concerns with the DCO or their line manager. This allows us to regularly review and strengthen the data protection measures that we have in place.

3 Compliance measures

3.1 The Schools help to ensure compliance with data protection law using the measures outlined at 4 to 13 below.

4 Training

4.1 All staff receive data protection training as part of their induction and refresher training is provided every two years as a minimum. The training is either online and staff must pass a test to complete the training **OR** delivered in person by the DCO, a member of the Operational Management Team or an external expert. In addition, staff awareness is sharpened with regular online testing.

4.2 The training includes (but is not limited to) the practical application of the UK GDPR's principles in a school context, guidance on how to keep personal data secure and when staff should speak to the DCO.

4.3 The Senior Leadership Team and governors receive additional training on an annual basis. This training has been specifically designed for their roles.

4.4 The DCO attends external training on a regular basis which is appropriate to their role as the senior individual who leads on the Schools' data protection compliance. This may be with data protection lawyers, online, etc.

4.5 Other teams and departments are given data protection training which is specific to their role or function as follows:

- Teaching Staff – on first appointment then annually with DCO or online with test.

- Pastoral Staff – on first appointment then every two years with DCO or online with test.
- Administration Staff – on first appointment then every two years with DCO or online with test.
- Marketing & Admissions Staff – on first appointment then every two years with DCO. Periodic training with data protection lawyers.
- Malvernian Society and Development Staff – on first appointment then every two years with DCO. Periodic training with data protection lawyers.
- Human Resources Staff – on first appointment then every two years with DCO.
- Finance Staff – on first appointment then every two years with DCO.
- Other Operational Staff – on first appointment with line manager.

5 Policies and guidance

5.1 All staff at the Schools are required to comply with the following documents:

5.1.1 Data Protection Policy: Practical Guidance for Staff;

5.1.2 Information Security Policy; and

5.1.3 Guidance for Staff on the Use of Photographs and Videos.

5.2 The DCO and Senior Management Teams are responsible for implementing the:

5.2.1 Data Breach Policy and Procedure;

5.2.2 Information and Records Retention Policy;

5.2.3 CCTV Policy; and

5.2.4 Appropriate Policy Document for special category personal data.

6 Documentation

6.1 Documenting how we comply with data protection law is a key part of our compliance. In addition to the documents listed at section 5 above we:

6.1.1 maintain a record of how we use personal data as required under Article 30 of the UK GDPR. The DCO is responsible for maintaining this record;

6.1.2 document our lawful bases for using personal data through our privacy notices;

6.1.3 keep a record of our legitimate interests assessments;

6.1.4 carry out risk assessments and when required a Data Protection Impact Assessment;

6.1.5 retain records of any consents obtained to use personal data by adding an entry to a Consent Register;

6.1.6 maintain a register of any data breaches. The DCO is responsible for completing this. All staff understand that they must inform the DCO of any suspected breach so that the register can be kept up to date;

6.1.7 record when staff complete data protection training to ensure that all staff have received the appropriate level of training; and

6.1.8 maintain an appropriate policy document regarding our processing of special category personal data and criminal offence data as required by the DPA 2018.

7 Privacy notices

7.1 The Schools have privacy notices, which are published on the Schools' websites.

7.2 We are mindful that some of our pupils are competent to exercise their own data protection rights. In light of this, we have developed a privacy notice for pupils which is age appropriate and addressed directly to the pupils.

7.3 In addition, the School explains how personal data will be used on a case by case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross refer to the applicable privacy notice.

8 Data protection by design and default

8.1 The School has built the data protection principles into its practices by implementing appropriate technical and organisation measures. This is known as data protection by design.

8.2 We also ensure that we only use the minimum amount of personal data to achieve our purposes - known as data protection by default.

8.3 More specifically we do the following:

8.3.1 at the start of any new project, or new activity, which involves using personal data (e.g. working with a new external activity provider, implementing new software or hardware) the DCO considers how we will comply with the data protection principles;

8.3.2 we make it clear on any data collection forms what personal data must be provided and what is optional;

8.3.3 we proactively consider data protection risks and adopt appropriate measures to protect personal data (e.g. encryption, physical security);

8.3.4 our external facing documents (e.g. privacy notices) are accessible and age appropriate;

8.3.5 before we share personal data externally we check that we have a lawful basis and that the sharing is fair;

8.3.6 we regularly review the measures which are in place to ensure that they are still appropriate;

8.3.7 we have developed a culture where staff understand the importance of data protection; and

8.3.8 if there has been a problem, or a "near miss", we will look at what has happened to improve our practices, for example, by providing additional staff training and awareness.

8.4 The Schools have various internal written procedures in place to comply with our obligations under the UK GDPR. This includes in relation to:

8.4.1 computer and network security;

8.4.2 the secure destruction of personal data - both electronic and paper copies;

8.4.3 individuals exercising their rights;

8.4.4 ensuring that we only use processors who comply with the UK GDPR; and

8.4.5 physical security when the School site is used by external parties.

8.5 The DCO determines whether a Data Protection Impact Assessment is required before the School begins any new type of processing activity. For example, before the School introduces new software to store pupil records.

9 Individuals' rights

9.1 We are committed to allowing individuals to exercise their rights under the UK GDPR. These rights are as follows:

9.1.1 right of access (i.e. making a subject access request);

9.1.2 right to rectification;

9.1.3 right to erasure;

9.1.4 right to restriction;

9.1.5 right to data portability; and

9.1.6 right to object.

9.2 Staff are trained to recognise when an individual is exercising a right under the UK GDPR and to pass this immediately to the DCO.

9.3 The Schools keep a log of all requests to exercise rights with the applicable deadline for our response. This log is maintained by the DCO.

9.4 To ensure that we meet our obligations the DCO or Head of HR co-ordinate our response to all requests. The DCO has detailed knowledge of how to respond to individuals' rights and has received external training. The DCO will involve other members of staff, as appropriate, in formulating the School's response.

9.5 Consideration is given to at least the following issues when responding to rights requests:

9.5.1 the importance of responding within the statutory timeframe, usually one calendar month (but this can be extended by up to two months for complex requests);

9.5.2 whether a pupil's consent should be sought before responding to their parent;

9.5.3 whether further engagement with the requester is needed, e.g. to ask for ID or to seek clarification of their request;

9.5.4 the exemptions under the Data Protection Act 2018;

9.5.5 the provision of supplementary information (e.g. sources and purposes) under a subject access request;

9.5.6 whether the request can be refused, or a reasonable fee charged, because it is manifestly unfounded or excessive; and

9.5.7 how to securely send our response to the requester.

10 Information security

10.1 The Schools have put in place technical and organisational measures to ensure the confidentiality, availability and integrity of personal data. The DCO is responsible for determining the appropriate organisational measures, for example, staff training and guidance.

10.2 The Head of ICT Services leads on the technical side of our information security, for example, network security. The Schools follow guidance from the National Cyber Security Centre and keep up to date with the latest cyber security news and alerts.

10.3 The Schools have implemented an Information Security Policy for staff.

10.4 We appreciate that prompt action is vital when handling information security incidents. Staff are trained to report any suspicions or concerns regarding potential personal data breaches to the DCO immediately.

10.5 The DCO will carry out an initial investigation and determine if the incident constitutes a personal data breach. If so, the procedure outlined in the Data Breach Policy and Procedure will be followed.

11 Processors

11.1 The Schools have procedures in place to check that the organisations acting as our processors are complying with the UK GDPR. The DCO] and Head of ICT Services are responsible for implementing these procedures.

11.2 The Schools have contracts in place with our processors which include the specific terms required by the UK GDPR. Legal advice is sought as required regarding these contracts.

11.3 Staff are trained to speak to the DCO if they need to share information with an organisation which may act as the School's processor so that the DCO can check that the appropriate measures are in place.

12 International transfers

12.1 The Schools maintain a record of when they transfer personal data outside of the UK and what safeguard or derogation is relied on under the UK GDPR. The DCO is responsible for maintaining this record.

12.2 Staff are trained to speak to the DCO before transferring personal data outside of the UK.

13 Data Protection Fee

13.1 The School has procedures in place to ensure that the data protection fee is paid to the Information Commissioner's Office for all controllers.

13.2 The PA to the Chief Operating Officer is responsible for ensuring the fee is paid on time.

14 Monitoring and review

14.1 The DCO will ensure that the content and implementation of the procedures set out in this policy are reviewed regularly.

14.2 Any personal data breaches at the School will be followed by a review of the relevant procedures by the DCO and a report made to the governors.

Date of Policy: 22 April 2023

Next review due: 22 April 2025

Policy Owner: Data Compliance Officer