MALVERNIAN
SOCIETY

Data Protection Policy

Introduction

1 **Introduction:** This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the Malvernian Society uses and stores information about identifiable people (**Personal Information**). It also gives you information about various rights regarding your information, such as the right to access the Personal Information about you that the Society holds.

2 **Lawful treatment of data:** The Society will collect, store and process Personal Information about our staff, former pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this information will maintain confidence in the Society and will ensure that the Society operates successfully.

3 **Application:** This policy is aimed at all staff working in the Society (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience, students and volunteers.

4 **Obligation:** You are obliged to comply with this policy when processing Personal Information on our behalf. Any breach of this policy may result in disciplinary action.

5 **Queries:** All queries concerning data protection matters should be raised with the Data Compliance Officer ,Mr David Angus: dataprotection@malcol.org (henceforward DCO) or, in his absence, the Bursar.

What information falls within the scope of this policy

6 **Data Protection:** Data protection concerns information about individuals.

7 **Personal Information:** Personal Information is information which relates to a living person who can be identified either from that information, or from the information and other information that is available. Information as simple as someone's name and address is their Personal Information.

8 **Personal Information at work:** In order for you to do your job, you will need to use and create Personal Information. Virtually anything might include Personal Information.

9 Examples of places where Personal Information might be found are:

9.1 on a computer database;

9.2 in a file, such as a personnel report;

9.3 in a register or contract of employment;

9.4 health records; and

9.5 email correspondence.

10 Examples of documents where Personal Information might be found are:

10.1 a record about disciplinary action taken against a member of staff;

10.2 photographs of former pupils;

10.3 a tape recording of a disciplinary hearing;

10.4 contact details and other personal information held about former pupils, current and former parents and staff and their families;

10.5 contact details of a member of the public who is enquiring about the archives;

10.6 information on a pupil's performance; and

10.7 an opinion about a parent or colleague in an email.

These are just examples; there may be many other things that you use and create that would be considered Personal Information.

11 **Categories of Critical Society Personal Information:** The following categories are referred to as **Critical Society Personal Information** in this policy. You must be particularly careful when dealing with Personal Information which falls into any of the categories below:

11.1 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

11.2 financial information (for example, about OMs and staff);

11.3 information about an individual's racial or ethnic origin;

11.4 political opinions;

11.5 religious beliefs or other beliefs of a similar nature;

11.6 trade union membership;

11.7 physical or mental health or condition;

11.8 sex life;

11.9 genetic information, and;

11.10 information relating to actual or alleged criminal activity.

If you have any questions about your processing of these categories of Critical School Personal Information please speak to the DCO.

Your obligations

12 **Personal Information must be processed fairly, lawfully and transparently**

12.1 What does this mean in practice?

12.1.1 'Processing' covers virtually everything which is done in relation to Personal Information, including using, disclosing, copying and storing Personal Information.

12.1.2 People must be told what information is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

12.2 This information is often provided in a document known as a Privacy Notice. Copies of the Society's Privacy Notices ('external' and for staff) can be obtained from the Operations Director or accessed on the Society's website. You must familiarise yourself with these notices.

12.3 If you are using Personal Information in a way which you think an individual might consider unfair please speak to the DCO.

13 **You must only process Personal Information for the following purposes:**

13.1 promoting events and activities (for example, OM reunions and sports fixtures);

13.2 protecting and promoting the Society's interests and objectives (for example, fundraising);

13.3 to fulfil the Society's contractual and other legal obligations.

14 **Use of Personal Information:** If you want to do something with Personal Information that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the DCO. This is to make sure that the Society has a lawful reason for using the Personal Information.

15 **Consent:** We may sometimes rely on the consent of the individual to use their Personal Information. This consent must meet certain requirements and therefore you should speak to the DCO if you think that you may need to obtain consent.

16 **You must only process Personal Information for limited purposes and in an appropriate way.**

16.1 What does this mean in practice?

16.1.1 For example, (in line with our Privacy Notice) if an OM is told that they will be photographed at a reunion, we would not normally use those photographs for another purpose (such as the development prospectus) without consent.

17 **Personal Information held must be adequate and relevant for the purpose.**

17.1 What does this mean in practice?

17.1.1 This means not making decisions based on incomplete information. For example, when writing 'pen-sketches' you must make sure that you are using all of the relevant information about the subject.

18 **You must not hold excessive or unnecessary Personal Information.**

18.1 What does this mean in practice?

18.1.1 Personal Information must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about an OM's siblings if that Personal Information has some relevance, such as allowing the Society to determine if a sibling should be invited to an event.

19 **The Personal Information that you hold must be accurate.**

19.1 What does this mean in practice?

19.1.1 You must ensure that Personal Information is complete and kept up to date. or example, if an OM notifies you that their contact details have changed, you should update the database.

20 **You must not keep Personal Information longer than necessary.**

20.1 What does this this mean in practice?

20.1.1 The Society has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting information.

20.1.2 The Information and Records Retention Policy the Document Retention Schedule can be found in the Staff Handbook.

20.1.3 Please speak to the DCO for any further guidance on the retention periods and secure deletion.

21 **You must keep Personal Information secure.**

21.1 You must comply with the following policies and guidance relating to the handling of Personal Information:

21.1.1 (Malvern College) Staff ICT Security & Acceptable Use Policy.

22 **You must not transfer Personal Information outside the EEA without adequate protection.**

22.1 What does this mean in practice?

22.1.1 If you need to transfer personal information outside the EEA please contact the DCO. For example, if you are arranging an OM reunion in a country outside the EEA.

Sharing Personal Information outside the Society office - dos and don'ts

23 **Dos and don'ts:** Please review the following dos and don'ts:

23.1 **DO** share Personal Information on a need to know basis: think about why it is necessary to share information outside of the Society office; if in doubt, always ask your line manager.

23.2 **DO** encrypt emails which contain Critical Society Personal Information described in paragraph 11 above. For example, encryption should be used when sending contact details of OMs for a rep to organise an event.

23.3 **DO** be aware of 'blagging'. This is the use of deceit to obtain Personal Information from people or organisations. You should seek advice from the DCO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from an OM but using a different email address).

23.4 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by

fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the ICT department.

23.5 **DO NOT** disclose Personal Information to the Police without permission from the Head of Malvern College (unless it is an emergency).

23.6 **DO NOT** disclose Personal Information to contractors without permission from the Estates Bursar, Domestic Bursar or Head of ICT Services as appropriate. This includes, for example, sharing Personal Information with an external marketing team to carry out a pupil recruitment event.

Sharing Personal Information within the School (taken from the Malvern College Data Protection Policy)

24 **Sharing Personal Information:** This section applies when Personal Information is shared within the wider school community., i.e. when Personal Information is shared between Malvern College and the Malvernian Society, Malvern College Enterprises or Malvern College International.

25 **Need to know basis:** Personal Information must only be shared within the school community on a 'need to know' basis.

Examples of sharing which are **likely** to comply with data protection legislation:

25.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);

25.2 informing an exam invigilator that a particular pupil suffers from panic attacks; and

25.3 disclosing details of a colleague's food allergy to colleagues in catering so that you/they will know how to respond.

Examples of sharing which are **unlikely** to comply with data protection legislation:

25.4 the Head being given access to all records kept by nurses working within the School (seniority does not necessarily mean a right of access);

25.5 giving all staff the full details of a fractious family problem rather than just signalling that extra care might be required; and

25.6 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

26 **Sharing of Personal Information and safeguarding**: You may share Personal Information to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the Designated Safeguarding Lead, Mrs Penny Bijl as a matter of urgency.

Individuals' rights in their Personal Information

27 **Rights:** People have various rights in their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the DCO.

28 **Individual's rights:** Please let the DCO know if anyone (either for themselves or on behalf of another person):

28.1 wants to know what information the Society holds about them;

28.2 asks to withdraw any consent that they have given to use their information or information about their child;

28.3 wants the Society to delete any information;

28.4 asks the Society to correct or change information (unless this is a routine updating of information such as contact details);

28.5 asks for electronic information which they provided to the Society to be transferred back to them or to another organisation;

28.6 wants the Society to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the OM Newsletter or alumni events information; or

28.7 objects to how the Society is using their information or wants the Society to stop using their information in a particular way, for example, if they are not happy that information has been used to invite them to events, or as part of a fundraising campaign.

Requests for Personal Information (Subject Access Requests)

29 **The right to request Personal Information:** One of the most commonly exercised rights mentioned in paragraph 27 above is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Information which the Society holds about them (or in some cases their child) and to certain supplemental information.

30 **Form of request:** Subject Access Requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states 'Please send me copies of all emails you hold about me' is a valid Subject Access Request. You must always immediately let the DCO know when you receive any such requests.

31 **If you receive a Subject Access Request:** Receiving a Subject Access Request is a serious matter for the Society and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

32 **Disclosure:** When a Subject Access Request is made, the Society must disclose all of that person's Personal Information to them which falls within the scope of the request; there are only very limited exceptions. There is no exemption for embarrassing information, so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

Breach

33 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

34 **Criminal Offence:** A member of staff who deliberately or recklessly discloses Personal Information held by the Society without proper authority is also guilty of a criminal offence.

updated 15 May 2018

to be reviewed May 2019.