THE ORATORY

Information Security Policy

This policy has been drafted to make staff aware of their obligations under both the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR), which replaced the Data Protection Act 1998 from 25 May 2018. Although the DPA 2018 and the GDPR now apply, there remains some uncertainty around their application, particularly as the ICO continue to publish new guidance. As such the document will likely need to be updated in due course.

1 Introduction

1.1 Information security is about what you and the Oratory School should be doing to make sure that **Personal Data** is kept safe. This is the most important area of data protection to get right. Most of the data protection fines have come about because of information security breaches.

1.2 The Oratory School (the **School**) is ultimately responsible for how you handle personal information.

1.3 This policy should be read alongside these policies which are relevant to data protection:

1.3.1 Privacy notices for staff, pupils and parents; and
1.3.2 IT acceptable use policy for staff.
1.3.3 Data Retention Policy

1.4 This policy applies to all staff (which includes Governors, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see the Schools Data Protection policy.

2 Be aware

2.1 Information security breaches can happen in a number of different ways.

Examples of breaches which have been reported in the news include:

2.1.1 an unencrypted laptop stolen after being left on a train;
2.1.2 Personal Data taken after website was hacked;
2.1.3 sending a confidential email to the wrong recipient.

2.2 These should give you a good idea of the sorts of things which can go wrong, but please have a think about what problems might arise in your department and what you can do to manage the risks. Speak to your line manager or the Bursar if you have any ideas or suggestions about improving practices in your department.

2.3 You should immediately report all security incidents, breaches and weaknesses to the Head Master or the Bursar. This includes anything which you become aware of even if you are not directly involved.

2.4 You must immediately tell Head Master, the Bursar and the IT Department if you become aware of anything which might mean that there has been a data protection or security breach. This could be anything which puts Personal Data at risk, for example, if Personal Data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen. All of the following are examples of a security breach:

2.4.1 you accidently send an email to the wrong recipient;
2.4.2 you cannot find some papers which contain Personal Data; or

2.4.3 any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

2.5 In certain situations, the School must report an information security breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

3 Assessments

3.1 In some situations, the School is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a particular risk to an individual's privacy.

3.2 These assessments should help the School to identify the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let the Bursar know.

4 Sensitive Data (Special Category Data)

4.1 Data protection is about protecting information about individuals. Even something as simple as a person's name or their hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called **Sensitive Data** in this policy and in the data protection policy but is now referred to as **Special Category Data** by the ICO. Sensitive Data is:

4.1.1 information concerning child protection matters;
4.1.2 information about serious or confidential medical conditions and information about special educational needs;
4.1.3 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);
4.1.4 financial information (for example about parents and staff);
4.1.5 information about an individual's racial or ethnic origin; and
4.1.6 political opinions;
4.1.7 religious beliefs or other beliefs of a similar nature;
4.1.8 physical or mental health or condition;
4.1.9 genetic information;
4.1.10 sexual life or sexual orientation;
4.1.11 information relating to actual or alleged criminal activity; and
4.1.12 biometric information (e.g. fingerprints used for controlling access to a building).

4.2 Staff need to be extra careful when handling Sensitive Data.

5 Minimising the amount of Personal Data that we hold

5.1 Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please refer to our Data Retention guidelines for the school.

6 Using computers and IT

6.1 A lot of data protection breaches happen as a result of basic mistakes being made when using School's IT system. Here are some tips on how to avoid common problems:

6.2 **Lock computer screens:** Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time. If you are not sure how to do this then speak to IT. The School's computers are configured to automatically lock if not used for a few minutes.

6.3 **Be familiar with IT:** You should also make sure that you familiarise yourself with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

6.3.1 if you use Microsoft Teams which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;
6.3.2 make sure that you know how to properly use any security features contained

in the Schools software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this software correctly so that the recipient of the document cannot "undo" the redactions; and

6.3.3 you need to be extra careful where you store information containing Sensitive Data. For example, safeguarding information should not be saved on a shared computer drive accessible to all staff.

6.4 **Hardware and software not provided:** Staff must not use, download or install any software, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the School's IT systems without permission.

6.5 **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share documents.

6.6 **Portable media devices:** The use of portable media devices (such as USB drives and portable hard drives) is not allowed unless those devices have been given to you by the School and you have received training on how to use those devices securely.

6.7 **IT equipment:** If you are given School IT equipment to use (this includes laptops, printers and phones) it must always be returned to the IT Department even if you think that it is broken and will no longer work.

7 Passwords

7.1 Passwords should be long and difficult to guess, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

7.2 You should not use a password which other people might guess or know, or be able to find out, such as your address or your birthday.

7.3 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

7.4 Passwords must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

7.5 Single sign-on (SSO) with your school credentials should be used for third party websites and applications where possible.

7.6 If it is not possible to use SSO with a third party website or application then you should unique password for each service you have registered with.

7.7 Multi-factor authentication should be configured to provide extra security for all services that offer it.

7.8 You can use the password management features in Microsoft Edge to store credentials for websites one devices managed by the school. Third party password managers should not be used.

8 Emails

8.1 When sending emails you must take care to make sure that the recipient/s are correct.

8.2 **Encryption:** All internal and external emails which contain Sensitive Data should be encrypted.

8.3 **Attachments:** Where possible a secure link to a document should be used rather than attaching the document to an email. If documents containing sensitive data must be attached to an email then they should be protected with either a password or rights management tools.

8.4 **Private email addresses:** You must not use a private email address for School related work. You must only use your school address. Please note that this rule applies to Governors as well.

9 Paper files

9.1 **Keep under lock and key:** Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

9.2 **Disposal:** Paper records containing Personal Data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal Data should never be placed in the general waste.

9.3 **Printing:** When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data then you must hand it in to the Bursar.

9.4 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Staff are provided with their own personal secure cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing any Sensitive Data.

10 Working off site (e.g. school trips and homeworking)

10.1 Staff might need to take Personal Data off the site for various reasons, (for example because they are working from home or supervising a school trip). This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

10.2 For school trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to the school.

10.3 If you are allowed to work from home then check with the Bursar what additional arrangements are in place. This might involve working with a specially encrypted memory stick or installing software on your home computer giving remote IT access to the School.

10.4 **Take the minimum with you:** When working away from your school you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with her information about pupil medical conditions (for example allergies and medication).

10.5 **Working on the move:** You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

10.6 **Paper records:** If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example:

10.6.1 documents should be kept in a secure place.

10.6.2 if travelling by train you must keep the documents with you at all times and they should not be stored in luggage racks;

10.6.3 if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights;

10.6.4 if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should usually take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you.

10.7 **Public Wi-Fi:** You must not use public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will either need to work offline or use 3G / 4G.

11 Using personal devices for school work

11.1 You may only use your personal device (such as your laptop or smartphone) for school work if you have been given permission by the School.

11.2 Even if you have been given permission to do so, then before using your own device for school work you must speak to your IT team so that they can configure your device.

11.3 **Appropriate security measures** should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

11.4 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should not be sent to or saved to personal devices, unless you have been given permission by the IT Department. This is because anything you save to your computer, tablet or mobile phone will not be protected by the Schools security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if you saved a school document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.

11.5 **Friends and family:** You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything school related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make sure that your devices are not configured in a way that would allow someone else access to school related documents and information – if you are unsure about this then please speak to the IT Department.

11.6 **When you stop using your device for school work:** If you stop using your device for school work, for example:

11.6.1 if you decide that you do not wish to use your device for school work; or
11.6.2 if the school withdraws permission for you to use your device; or
11.6.3 if you are about to leave

then, all school documents (including school emails), and any software applications provided by us for school purposes, will be removed from the device.

If this cannot be achieved remotely, you must submit the device to the IT

Department for wiping and software removal. You must provide all necessary co-operation and assistance to the IT department in relation to this process.

12 Breach of this policy

12.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

12.2 A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in dismissal in accordance with our Staff Code of Conduct.

12.3 This policy does not form part of any employee's contract of employment.

12.4 We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes.

13 Data Protection Officer

The Data Protection Officer is responsible for overseeing data protection within the School so if you do have any questions in this regard, please do contact them on the information below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with us before involving them.

I confirm that I have read and understood the contents of this policy:

Name	.....
Signature	.....
Date	_____Date/_____month/_____year