Date March 2021
Review Date March 204
Responsibility Bursar

Information Security Policy

1 Introduction

1.1 Information security is about what you and the College 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 This policy should be read alongside the College's Data Protection Policy which gives an overview of your and the College's obligations around data protection. The College's Data Protection Policy can be found **here**. In addition to the Data Protection Policy, you should also read the following which are relevant to data protection:

1.2.1 the College's Privacy Notices for Staff, Pupils and Parents;

1.2.2 Record Management Policy; and

1.2.3 Staff ICT Acceptable Use Policy.

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

1.4 Any questions or concerns about your obligations under this policy should be referred to the Bursar. Questions and concerns about technical support or for assistance with using the College IT systems should be referred to the IT Department.

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; and

2.1.4 Leaving confidential documents containing personal data on a doorstep.

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 team or department and what you can do to manage the risks. Speak to your manager and the Bursar if you have any ideas or suggestions about improving practices in your team. One option is to have team specific checklists to help ensure data protection compliance.

2.3 You should immediately report all security incidents, breaches and weaknesses to the Bursar. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends).

2.4 You must immediately tell the Bursar and the IT Department if you become aware of anything which might mean that there has been a security breach. You must provide your manager or the Bursar with all of the information you have. If you cannot get hold of your manager or the Bursar or it is outside of school hours then please use this emergency contact number – 07876 501781. 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 College 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 Thinking about privacy on a day to day basis

3.1 We should be thinking about data protection and privacy whenever we are handling Personal Data. If you have any suggestions for how the College could protect individual's privacy more robustly please speak to the Bursar.

3.2 From May 2018, the College 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 risk to individual's privacy or where Personal Data is used on a large scale, such as CCTV.

3.3 These assessments should help the College 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 Critical College Personal 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 **Critical College Personal Data** in this policy and in the data protection policy. Critical College Personal 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 trade union membership;

4.1.9 physical or mental health or condition;

4.1.10 genetic information;

4.1.11 sexual life;

4.1.12 information relating to actual or alleged criminal activity; and

4.1.13 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

4.2 Staff need to be extra careful when handling Critical College Personal 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. If you would like guidance on when to delete certain types of information please speak to the Bursar.

6 Using computers and IT

6.1 A lot of data protection breaches happen as a result of basic mistakes being made when using the College'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. To lock your computer screen, press the "Windows" key followed by the "L" key. If you are not sure how to do this then speak to IT. The College's computers are configured to automatically lock if not used for five minutes in the case of pupils and fifteen minutes for staff.

6.3 **Be familiar with the College's 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 a "virtual classroom" 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 College 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 Critical College Personal Data. For example, safeguarding information should not ordinarily be saved using alumni database software. If in doubt, speak to the Bursar.

6.4 Specific guidance on the information security requirements of the different programmes that the College uses can be found in the Appendix 1 to this policy.

6.5 **Hardware and software not provided by the College:** 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 College IT systems without permission.

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

6.7 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) to store Personal Data is not allowed unless those devices have been encrypted. The IT Department can provide further advice in this respect.

6.8 **Disposal of College IT equipment:** College IT equipment (this includes laptops, printers, phones, and DVDs) 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, 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 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might 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 (and any other security credential you are issued with such as a key fob or USB drive) 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 Staff will be required to change their password every half a term. The new password must follow the College's policy: it must not be the same as any of the previous six passwords, must be a minimum of 8 characters and have at least 3 different characters (i.e. upper case, lower case, number or special characters).

8 Emails (and faxes)

8.1 When sending emails or faxes you must take care to make sure that the recipients are correct.

8.2 **Emails to multiple recipients:** If the email or fax contains Critical College Personal Data then you should ask another member of staff to double check that you have entered the email address / fax number correctly before pressing send. If a fax contains Critical College Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.3 **Encryption:** Remember to encrypt internal and external emails which contain Critical College Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. Please speak to the IT Department if you need assistance in encrypting emails. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password.

8.4 **Private email addresses:** You must not use a private email address for College related work. You must only use your @epsomcollege.org.uk address. Personal use of College email addresses should be limited, as outlined in the Staff ICT Acceptable Use Policy.

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 If the papers contain Critical College Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (**DSL**) office. These are special cabinets used by the College which are kept in a secure location. They are also too heavy to move to minimise the risk of theft. The cabinets are located around the College as follows:

Cabinet	**Access**
Child protection - located in the DSL's office	The DSL is the main key holder for the locked cabinets in his office, and the key is kept securely on his person at all times. The Bursar has a spare key for use in an emergency.
Financial information - located in Accounts Office and Corridor	Kept in locked cupboards. Members of the Accounts Department have access to the keys which are kept in a locked key cabinet.
Health information and staff data	Kept in a locked cupboard in the HR office. This is locked when not occupied during the day, and alarmed overnight/during the weekend. Keys are only held by the three members of the HR Department.

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins which are located in the Photocopying Room, HR Department or Bursar's Office. Personal Data should never be placed in the general waste.

9.4 **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. The College uses "follow me" printing which means that you cannot print something out unless you are standing by the printer.

9.5 **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 Critical College Personal Data. Please see paragraph 9.2 above for details of where Critical College Personal Data should be kept.

9.6 **Post:** You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking your IT team to put in on an encrypted memory stick or arrange for it to be sent by courier.

10 Working off site (e.g. College trips)

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

10.2 For College trips, the trip organiser, in conjunction with the External Visits Coordinator 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 College.

10.3 **Take the minimum with you:** When working away from the College 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). If only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.

10.4 **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.

10.5 **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:

10.5.1 documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);

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

10.5.3 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;

10.5.4 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 (please see paragraph 10.3 above).

10.6 **Public Wi-Fi:** Staff should take care when using public Wi-Fi to connect to the internet. Wherever possible they should not use public Wi-Fi if they are working on anything that contains personal data.

10.7 Critical College Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for school trips (see 10.3 above).

11 Using personal devices for College work

11.1 **Using your own PC or Laptop:** It is acceptable to use your laptop or PC to access College information stored in the cloud (e.g. OneDrive) but if you want to connect for College systems then you can only do so by using the College's remote access software. Using this system means that Personal Data is accessed

through the College's own network which is far more secure and significantly reduces the risk of a security breach.

11.2 **Appropriate security measures** should always be taken. This includes the use of anti-virus software. Any software or operating system on the device should be kept up to date. The College uses a Network Access Policy (NAP) to ensure that any device connected to the College's network has up-to-date anti-virus software installed on it.

11.3 **Default passwords**: If you use a personal device for school work which came with a default password then this password should be changed immediately. Please see section 7 above for guidance on choosing a strong password.

11.4 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should not normally be sent to or saved to personal devices, unless you have been given permission by the Second Master. This is because anything you save to your computer, tablet or mobile phone will not be protected by the College's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if you saved a College 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 College 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 College work:** If you stop using your device for College work, for example:

11.6.1 if you decide that you do not wish to use your device for College work; or

11.6.2 if the College withdraws permission for you to use your device; or

11.6.3 if you are about to leave the College

then, all College documents (including College emails), and any software applications provided by us for College 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 discloses Personal Data held by the College without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

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 by mail or email.

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

Name	……
Signature	……
Date	

Appendix 1 College applications

Application	What it can be used for	Specific security arrangements	Any other notes / comments
iSAMS	Storing pupil and parental information	Only those staff who require access to iSAMS as part of their role are granted access. Different permissions levels ensure that staff only have access to the appropriate level of detail to enable them to carry out their role.	Cloud based backup
Badger	Managing day to day operation of pastoral care for pupils	HMM and Matron have access to their house specific data. Only Headmaster and Second Master have access to information from all houses	Access by other staff to Badger can only be authorised by the Second Master or Bursar
CPOMS	Managing safeguarding matters	Only the Headmaster, Second Master (DSL) and Assistant Head: Pupil Welfare have access. Specific access relating to particular pupils is given to HMMs or Deputy DSL's as deemed necessary by the DSL	
Sage	Recording all financial transactions, including payroll, fee payments and purchase ledger.	Only members of the Accounts Department and the Bursar have access to Sage. Budget holders can only review their individual budgets, but cannot make any entries.	Cloud based backup
HR Database (Access database)	Storing staff information including emergency contract details, sickness records and all information required to maintain the Single Centralised Register	Access only granted to those who need it as part of their roles and responsibilities.	Cloud based backup
InTouch (Alumni Database)	Storing information on current pupils, alumni, ex-parents and ex-staff and current parents	Only the OE Club Secretary, the Archives Department, and Education Trust Department members have permission to access the database. Different staff have different permission levels.	

Evolve	Cloud based, reads personal information (names, contact details for pupils, parents etc.) from iSAMS.	Only dedicated application managers have access to all information in Evolve. All teachers can access data stored on pupils although this data is the same as in iSAMS.	
Parent evening system	Cloud based. Reads personal information on all current staff and current pupils, teaching sets, teaching forms from iSAMS	Only dedicated application managers have access to all information. All teachers can access data stored on pupils although this data is the same as in iSAMS.	
Room booking system	Cloud based. Reads from iSAMS information on all buildings and rooms, all current staff personal data and academic timetable.	Only dedicated application managers have access to all information. All teachers can access data stored on pupils although this data is the same as in iSAMS.	
SOCS	Cloud based. Reads pretty much all relevant information stored in iSAMS.	Only dedicated application managers have access to all information. Other users like teachers, students and parents can read only published information like College calendar, sport fixtures etc.	
Booking Live	Booking of holiday courses and events	Only those staff who require access to Booking Live as part of their role are granted access.	
Sage Pay	Card transitions	Only those staff who require access to Sage Pay as part of their role are granted access; commercial team and accounts.	PCI DSS compliant Validation date 25 January 2018