Staff Information Security Policy

Including all of the Pre-Prep Department and Early Years Foundation Stage

DJJK

Oct 2020

Review and Amendment Record

Date	Person Conducting the Review	Changes Made
Mar 2018	PMS	New for GDPR
May 2018	DJJK	
Oct 2018	DJJK	Review
Oct 2019	Ops Dir	Annual Review
Oct 2020	Ops Dir	Annual Review

1 **Introduction**

1.1 Information security is about what you and the 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 This policy should be read alongside the School's GDPR Policy for Staff, which gives an overview of your and the School's obligations around data protection. You should also read the following which are relevant to data protection:

1.2.1 the School's Privacy Notices for staff, pupils and parents; and

1.2.2 Technology & Acceptable Use Policy for staff.

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 School's Data Protection policy for staff. The policy applies to Prep, Pre-prep and EYFS.

1.4 Any questions or concerns about your obligations under this policy should be referred to Operations Director. Questions and concerns about technical support or for assistance with using the School 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;

2.1.4 leaving confidential documents containing Personal Data on a doorstep; and

2.1.5 using carbon copy (cc) rather than blind carbon copy (bcc) to send emails to multiple recipients.

2.1.6 using someone else's account to access systems.

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 line manager or the Operations Director 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 a member of your School Senior Management Team or the Operations Director. 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 a member of your Senior Management Team or the Operations Director if you become aware of anything which might mean that there has been a security breach. You must provide colleagues with all of the information you have. If it is outside of school hours then please use the emergency contact numbers you have for your school – do not wait, report immediately, no matter what time of day it is or if the school is closed. 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 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 School could protect individuals' privacy more robustly, please speak to Operations Director.

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

3.3 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 Operations Director know.

4 School 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 School Special Category Data in this policy and in the data protection policy. School Special Category 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 must be extra careful when handling School Special Category 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 Operations Director.

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 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. To lock your computer: Press Ctrl/Alt/Del and select Lock Workstation. The School's computers are configured to automatically lock if not used for fifteen minutes except in Pre Prep where there is a different timing.

6.3 **Be familiar with the School'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 School 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 School Special Category Data. For example, safeguarding information should not ordinarily be saved using alumni database software. If in doubt, speak to the Operations Director.

6.4 Specific guidance on the information security requirements of the different programmes that the School uses is available from the IT Department.

6.5 **Hardware and software not provided by the School:** 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 any School IT systems other than the WiFi network accessed using the personal key provided without permission.

6.6 **Using new software or digital service:** If you would like to use a digital service such as an online platform, app or piece of software for the first time, you will need to confirm if it complies with Data Protection law and it is safe to use. The requirement and tracking of confirmation is completed by the Bursary.

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

6.7 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) should be kept to a minimum. If you have to use one, it must be encrypted - the ICT Department will be able to offer advice on this.

6.8 **Disposal of School IT equipment:** School IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the IT Department for disposal 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. 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.

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:** A blind carbon copy (bcc) function must be used when sending emails to multiple email recipients (more than 2) outside the School email system so that names and email address are not visible to other recipients.

8.3 If the email or fax contains Critical School 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 School Personal Data, then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.4 **Encryption:** Remember to encrypt internal and external emails which contain School Special Category Data. For example, encryption should be used when sending details of a safeguarding incident to social services. If you need help encrypting a file, please raise an IT request or call the ICT Network Manager. 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.

8.5 **Private email addresses:** You must not use a private email address for School related work. You must only use your @summerfields.com address.

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 School Special Category Data, then they must be kept in secure cabinets and kept in a secure location.

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by either placing them in confidential waste bags under coordination of the School Office or through shredders. 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 a member of your Senior Management Team.

9.5 **Scanning**. When scanning documents please ensure that they are sent to an appropriately secure location on the network.

9.6 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Staff must keep papers containing personal data in locked drawers or cabinets.

9.7 **Post external:** 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 the ICT team to put it on an encrypted memory stick or arrange for it to be sent by courier. All such envelopes must be marked “Private and Confidential” and contain a return to sender address

9.8 **Post internal**: You must be careful when sending personal data around the school. It must be in a sealed envelope marked “Private and Confidential”. School Special Category Data must be delivered by hand and again in a sealed envelope and marked “Private and Confidential.

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

10.1 Staff might need to take Personal Data off the School 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 **Take the minimum with you:** When working away from the 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). 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.

10.3 **Working on the move:** You must not work on documents containing any 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.

10.4 **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:

10.4.1 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);

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

10.4.3 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;

10.4.4 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 10.2 above).

10.4.5 School Special Category 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 above).

10.5 **Public Wi-Fi:** You must not use public Wi-Fi to connect to the internet when using School devices and/or when accessing remote systems containing personal information. 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 use your personal device (such as your laptop or smartphone) for School work but this must be secure and encrypted.

11.2 Please refer to the taking images policy for using personal devices for photographic purposes.

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 **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.

11.5 **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 IT Department. This is because anything you save to your computer; tablet or mobile phone will not be protected by the School'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 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.

11.6 **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 must 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 ICT Department.

11.7 **When you stop using your device for School work:** If you stop using your device for School work, for example:

11.7.1 if you decide that you do not wish to use your device for School work; or

11.7.2 if the School withdraws permission for you to use your device for work purposes; or

11.7.3 if you are about to leave the School

then, all School documents (including School emails), and any software applications provided by us for School purposes must be removed from the device. The ICT Department will assist if needed. You must provide all necessary co-operation and assistance to the ICT 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 School 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 of staff member

Signed

Date

Circulation for comment and input:

Headmaster, Deputy Headmaster, Operations Director, Finance Director, External Relations Director, HR Manager, Finance Manager, Domestic Bursar, Head Sister, Director of Studies, Designated Safeguarding Lead, Head of Pastoral Care. Operations Director.

Publication:

School website and school policy folder.