**GDPR Information Security Policy (Staff)**

1. **Introduction**
	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.
	2. This policy should be read alongside the School's Data Protection Policy which gives an overview of your and the School's obligations around data protection. The School's data protection policy can be found at www.stowe.co.uk/policies. In addition to the data protection policy, you should also read the following documents which are relevant to data protection:
		1. the School's privacy notices for staff, pupils and parents; and
		2. IT Acceptable Use Policy for staff.
	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.
	4. Any questions or concerns about your obligations under this policy should be referred to the Privacy Officer by contacting PrivacyOfficer@Stowe.co.uk. Questions and concerns about technical support or for assistance with using the School IT systems should be referred to support@stowe.co.uk.
2. **Background concerning information security at Stowe**
	1. Information security breaches can happen in a few different ways. Examples of breaches which have been reported in the news include:
		1. an unencrypted laptop stolen after being left on a train;
		2. personal data taken after a website was hacked;
		3. sending a confidential email to the wrong recipient; and
		4. leaving confidential documents containing Personal Data on a doorstep.
	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 Privacy Officer PrivacyOfficer@Stowe.co.uk, 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.
	3. You should immediately report all security incidents related to personal data to the Privacy Officer PrivacyOfficer@Stowe.co.uk. 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.
	4. You must immediately email the Privacy Officer if you become aware of anything which might mean that there has been a data protection breach. If it is outside school hours then please also phone the Security team on 01280 8188228 and ask them to call the Privacy Officer as soon as possible. Examples of incidents include:
		1. you accidently send an email to the wrong recipient and sensitive data might be at risk of leaking beyond the control of Stowe School.
		2. papers which contain Personal Data are lost and are beyond the control of Stowe school.
		3. any device (such as a laptop or a smartphone) used to store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.
	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**
	1. We should be thinking about security and privacy whenever we are handling Personal Data. If you have any suggestions for how the School could protect individual's privacy more effectively please inform the Privacy Officer. (PrivacyOfficer@Stowe.co.uk)
	2. 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 individual's privacy or where Personal Data is used on a large scale, such as CCTV.
	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 the Privacy Officer know.
4. **Critical School Personal Data**
	1. 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 School Personal Data** in this policy and in the Data Protection Policy. For this reason, this data should only be stored or ‘saved’ on devices which are encrypted and password protected with a screen lock.
	2. Staff need to be extra careful when handling Critical School Personal Data.
	3. Critical School Personal Data includes the following categories of information related to an individual:
		* + information concerning child protection matters;
			+ information about serious or confidential medical conditions and information about special educational needs;
			+ 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);
			+ financial information (for example about parents and staff);
			+ information about an individual's racial or ethnic origin; and
			+ political opinions;
			+ religious beliefs or other beliefs of a similar nature;
			+ trade union membership;
			+ physical or mental health or condition;
			+ genetic information;
			+ sexual life;
			+ information relating to actual or alleged criminal activity; and
			+ biometric information (e.g. a pupil's fingerprints held for door access control).
5. **Minimising the amount of Personal Data that we hold**
	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 Privacy Officer.
6. **Using computers and IT**
	1. A lot of data protection breaches happen because of basic mistakes being made when using the School's IT system. Here are some tips on how to avoid common problems:
		1. **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.
		2. **Be familiar with the School's IT:** You should also make sure that you familiarise yourself with any software or hardware that you use. Please make sure that you understand what the software is supposed to be used for and any risks. For example:
		3. if you use "Stowenet" or MS Office 365 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.
		4. make sure that you know how to properly use any security features contained in School software required for your role. 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
		5. you need to be extra careful where you store information containing Critical School Personal Data. For example, safeguarding information should not be treated with additional caution. If in doubt, speak to the Privacy Officer.
	2. **Hardware and software not provided by the School:** Staff must not use, download or install any software, app, programme, or service without approval from the Privacy Officer. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any unapproved type of device or hardware to the School IT network without authorisation from the IT dept.
	3. **Private cloud storage:** Staff must not use private cloud storage or file sharing accounts to store or share School documents.
	4. **Mobile Phones and Portable media devices:** Devices must be protected with encryption. By default, secure school services should be used for data storage.
	5. **Return/Disposal of School IT equipment:** School 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.
	6. **Passwords**
		1. Passwords should be longer than or equal to 12 characters. For example, you could use a song lyric or a memorable phrase. Do not choose a password which is so complex that it's difficult to remember without using a password manager. Your password should not be disclosed to anyone else.
		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 name/birthday.
		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. **Emails (and faxes)-**
		1. When sending emails or faxes you must take care to make sure that the recipients are correct.
		2. **Emails to multiple recipients:** E-mail distribution groups are enabled on request to the Group Director of ICT. The update and management of constituents is the responsibility of the sponsor, usually the senior leader within that group. Access to the use of the ‘all staff’ e-mail group is restricted, though can requested through the Reception team. Parents can be emailed through the MIS system.
		3. If an email or fax contains sensitive Personal Data it is good practice to ask a colleague to double check that you have got all the details and recipient information correct before pressing send, and that the recipient is waiting at the receiving device.
	8. **Storing or sharing Critical School Personal Data.**
		1. Encryption must be used when storing or sending critical data. If data is sent externally the recipient organisation must be approved by the Data Protection Officer and emails/documents containing personal data must be password protected and encrypted. To use encryption, contact IT Support for help. Please note if you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a safe, separate communication. For example, after emailing the encrypted documents you may wish to call the recipient to tell them the password.
	9. **Private email addresses:** You must not use a private email address for email related to work.
	10. **Paper files**
		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.
		2. **Cabinets:** If the papers contain Critical School Personal Data then they must be kept in secure cabinets identified for the specified purpose. 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) room. These are special cabinets used by the School which are fire proof and are kept in a secure location. They are also too heavy to move to minimise the risk of theft.
		3. **Disposal:** If not shredded, paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins which are located in the General Office or by arranging for a secure bin collection from the Security team. Personal Data should never be placed in the general waste.
		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 Privacy Officer. Printing should only be completed in the same room unless a ‘print release printer’ is used and released when the publisher is by the outputting printer.
		5. **Put papers away:** You should always keep a tidy desk and put papers with Personal Data in them away when they are no longer needed. Where required Staff will be provided with their own personal cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing Critical School Personal Data. Please see paragraph 6.10.2 above for details of where Critical School Personal Data should be kept.
	11. **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 it on an encrypted memory stick or arrange for it to be sent by courier.
	12. **Working off site (e.g. School trips and homeworking)**
		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.
		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.
		3. **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 printed 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.
		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 must not leave any device unattended where there is a risk that it might be taken. All Devices must be password protected and encrypted.

* 1. You must not use non password protected public Wi-Fi to connect to the internet and only secure HTTPS should be used for the processing of personal data. For example, if you are working in a cafe and cannot be sure of a secure connection, then you will either need to work offline or use 5G / 4G.
	2. **Using School laptops, phones, cameras and other devices:** If you need to book out a School device then please contact ICT Support on support@stowe.co.uk at least 4 days in advance.
1. **Using personal devices for School work**
	1. You may only use your personal device (such as your laptop or smartphone) for School work if:
		1. you are accessing marking and creating lesson materials that do not contain sensitive personal materials or altering on-line materials.
		2. you utilise data and applications within Microsoft 365 or other remote services such as iSams using your browser and do not store data on the device.
		3. your phone/device must be auto locked when not in use and require a password in order to access it (see 11.4 below)
	2. Loss or theft of devices.
		1. Loss or theft of any device with school data on it must be reported to the ICT dept. The School reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for the School or on the School's behalf or which contains Personal Data. Although we do not intend to wipe other data that is private in nature (such as private photographs or private files or emails), it may not be possible to distinguish all such information from Personal Data.
	3. **Default passwords:** If you use a personal device for schoolwork which came with a default password then this password should be changed immediately. Please see section 6.5 above for guidance on choosing a strong password.
	4. **Sending or saving information to your personal devices:**
		1. Pictures or video can be temporarily captured and stored on an encrypted device but must then be moved to your One Drive/Office 365 account within 7 days. This is because anything you save to your computer, tablet or mobile phone will not be protected by the School's security systems.
		2. You should use the MS 365 online service without downloading a local copy.
	5. **Friends and family:**
		1. 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.
	6. **Keeping school related personal data off your personal devices:**
		1. If you have any personal data on your personal devices, either authorised or otherwise and:
			* 1. if you decide that you do not wish to use your device for School work; or
				2. if the School withdraws permission for you to use your device; or
				3. if you are about to leave the School

then, all School documents (including School emails), and any software applications provided by Stowe for School purposes, must be removed from the device. If you have downloaded software from the school please remove it and inform the ICT department if you have any issues.

* 1. **Breach of this policy**
		1. Any breach of this policy will be taken seriously and may result in disciplinary action.
		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.
		3. This policy does not form part of any employee's contract of employment.
	2. We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.