STOCKPORT GRAMMAR SCHOOL

INFORMATION SECURITY POLICY

(Reviewed by Governors 16.10.18)

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 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 on the School intranet at T:\All Staff\POLICIES. In addition to the data protection policy, 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 IT acceptable use policy for staff.

1.2.3 The School's policy for taking using and storing images

1.2.4 TBC Records and retention

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.

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 School IT systems should be referred to the ICT Helpdesk.

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 Head of Department/Line Manager or the Bursar if you have any ideas or suggestions about improving practices in your department. One option is to have department 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 ICT Helpdesk if you become aware of anything which might mean that there has been a security breach. You must provide your Head of Department/Line Manager or the Bursar with all of the information you have. If you cannot get hold of your Head of Department/Line Manager or the Bursar or it is outside of school hours then please use the SMT emergency contact number 07860 430754. Staff in the Junor School should contact the Headmaster of the Junior School. 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 as to how the School could protect individual's privacy more robustly please speak to the Bursar.

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 particular risk to an individual's privacy.

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 the Bursar know.

4 Critical School Personal Data

4.1 Data protection is about protecting information about individuals. Even something as simple as a person's name, address or interests 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. Critical School 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;

4.1.6 information about an individual's political opinions;

4.1.7 information about religious beliefs or other beliefs of a similar nature;

4.1.8 information about an individual's trade union membership;

4.1.9 information about an individual's physical or mental health or condition;

4.1.10 information about an individual's genetic information;

4.1.11 information about an individual's sexual life;

4.1.12 information relating to actual or alleged criminal activity; and

4.1.13 biometric information (e.g. fingerprints used for controlling access to a building).

4.2 Staff need to take additional care when handling Critical School 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 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 screen press the "Windows" key followed by the "L" key. If you are not sure how to do this then speak to IT.

6.3 **Be familiar with the School's ICT:** 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 you need to be extra careful where you store information containing Critical School Personal Data. For example, detailed safeguarding

information should not be saved in an area that is accessible by all staff. If in doubt, speak to Designated Safeguarding Lead or Bursar.

6.4 Specific guidance on the information security requirements of the different programmes that the School is available from the ICT Helpdesk.

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 ICT 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 IT systems without permission.

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,) 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. The ICT Helpdesk will give guidance on how to encrypt any portable media device.

6.8 **Disposal of School IT equipment:** School ICT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the ICT Helpdesk 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 You will be asked to change your password on a regular basis; the ICT team will notify you of the timing of this.

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:** Ensure that you only use custom groups set up from iSAMS to send emails to multiple recipients. Try to avoid replying to emails that have multiple addresses included. The School office can assist in sending out group emails or guidance is available from the ICT Helpdesk.

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 Critical School Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption then you need to speak to the ICT Helpdesk who will explain how to do this. 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 @stockportgrammar.co.uk address. Please note that this rule applies to Governors as well. Please speak to the ICT Department if you require an email account to be set up for you.

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 School 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 locked cabinets in the offices of the Designated Safeguarding Leads (**DSLs**). The cabinets are located around the School as follows:

Cabinet	**Access**
Child protection - located in the DSLs offices	Each cabinet should be kept secure at all times. DSL's should control who has access to keys and a spare key must always be held in the Bursary safe for emergency access.
Financial & HR information - located in the Bursary and Headmasters' offices	Each cabinet should be kept secure at all times. Access to keys should be restricted to the relevant staff and a spare key must always be held in the Bursary safe for emergency access.
Medical and SEND information	Each cabinet should be kept secure at all times. Access to keys should be restricted to the relevant staff and a spare key must always be held in the Bursary safe for emergency access.

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bags which are available on request from the Bursary. Personal Data should never be placed in the general waste.

9.4 **Printing:** When printing documents, make sure that you collect everything particularly from a network 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 School Office. The School's printing facility for shared printer requires staff to use their access card to retrieve material sent to a shared device using "Papercut" software

9.5 **Put papers away:** You should always keep a tidy desk and put papers containing personal data away when they are no longer needed. Please see paragraph 9.2 above for details of where Critical School Personal Data should be kept.

9.6 **Post:** You also need to take additional care when sending items in the post. Confidential materials should not be sent using standard post; consider if it can be encrypted and sent electronically or whether it should be sent as tracked post.

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 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 working from home access to School data is via Citrix which is the School's secure network. Staff can access emails on other portable devices (see 10.6 below).

10.4 If in doubt about the arrangements for working from home speak to your Head of Department/Line manager or the Bursar.

10.5 **Review the amount of information to take with you:** When working away from the School you must only take the relevant amount of information with you and try to keep this to a minimum.

10.6 **Working on the move:** You must not work on documents containing Personal Data whilst travelling or away from School 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, 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.

10.7 **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:

10.7.1 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);

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

10.7.3 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;

10.7.4 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 10.5 above).

10.8 **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.

10.9 **Using School laptops, phones, cameras and other devices:** If you need to book out a School device then this should be requested in advance from the ICT helpdesk

10.10 Critical School 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 10.5 above).

11 Using personal devices for School work

11.1 You should only use your personal device (such as your laptop or smartphone) for School work if you are not using sensitive personal data.

11.2 Guidance on how to access school services from a home computer or portable device is contained in Appendix 1 of this policy.

11.3 If you are using a home computer, please ensure that you use a dedicated user account that no other users can have access to

11.4 If you are using a portable device to access via Citrix please ensure that you do not automatically store your password within the app.

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

11.6 **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.

11.7 **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 your Head of Department/Line Manager or member of the Senior Management Team. 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.

11.8 **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 ICT Helpdesk.

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

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

11.9.2 if the School withdraws permission for you to use your device; or

11.9.3 you are planning to dispose of an old piece of equipment; or

11.9.4 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.

If this cannot be achieved remotely, you must submit the device to the ICT Helpdesk for wiping and software removal. You must provide all necessary co-operation and assistance to the ICT Helpdesk 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.

Appendix 1

Citrix Storefront / Workspace

If accessing school services using your home computer (whether it is a pc, mac, laptop, MacBook or something else) please ensure that you are using a dedicated user account that other users in the home do not have access to.
On Windows 10, a good explanation of how to do this and the reasons why can be found here.

On portable devices such as tablets or smartphones, multiple user accounts are not always an option. If you are using Citrix on one of these devices then please ensure that you do not store your password within the app. This means that your credentials will not automatically be filled in when accessing the Citrix app.

Web-based School Services

The school offers direct browser-based access to a number of services.
These include, but are not limited to:

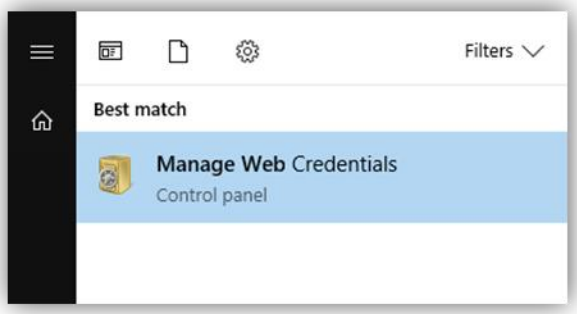
iSAMS;
Outlook Web Access (OWA);
Office 365;
Citrix Storefront (light version);
SGS Online
FoldR

As there is a large amount of potentially confidential and sensitive data that can be accessed using these services, it is important that we do as much as we can to make sure that our access is secure.

If you access any of these services directly through the browser on your tablet, smartphone or home computer, it is important that you do not store your credentials in your browser.
This is easy to spot as it means the browser will autofill the boxes without you having to re-enter your username and/or password every time.

If this happens, then there are ways to clear the stored credentials…

If you use Microsoft Edge or Internet Explorer on Windows 10, you can do this by simply searching for 'Manage Web Credentials'.
This shows you a list of each web based login that you have stored on your pc – simply delete each entry as required.

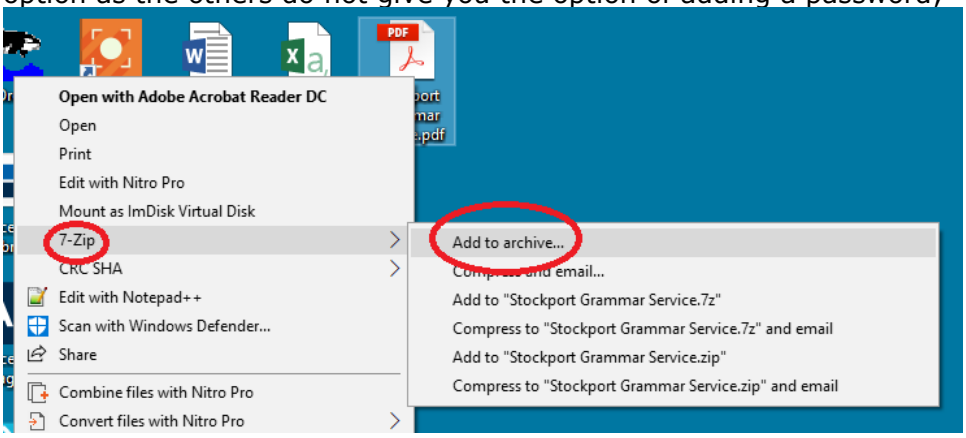


If you use Google Chrome, simply type **chrome://settings/passwords** into your Chrome address bar to see a similar list of stored logins. Other browsers have similar ways of checking the stored credentials.

Data stored on personal devices

Any documents that contain potentially sensitive or personal data, pupil or otherwise, must be treated in a secure manner.
It is always preferable to access any documents of this type from either within school on a school computer or remotely through Citrix.
If the need arises when you absolutely must work on a document containing school data remotely and Citrix is not available, it is advisable that you do not actually transfer the document to your own device but instead keep it on either your school OneDrive of Google Drive. Documents held on these drives can be accessed on most devices from anywhere where you have an internet connection, and can be edited from within the browser without the need to download the document to your own device.
If this is still not an option, such as when you have to work on a document and you know that you will be completely offline, please ensure that the document is secure within an encrypted zip.
To do this from a school computer…

1) Right click on the required files or folder (you can select multiple items);
2) Select 7-Zip ☐ Add to archive… It is important that you choose this option as the others do not give you the option of adding a password;



3) Select the location and name of the zip file – the default is the location you are currently in and is probably fine;
4) Type in whatever password you desire;
5) Click OK!

Please note – once set you cannot change or remove the password, you have to create a new zip file if you want to do this.

Email on Mobile Devices

Many staff now have their school email on their smartphones. This uses as technology known as Exchange Activesync and means that the school emails are downloaded onto the mobile device. Although this can be very useful, it is also a potential security risk.

If you do have your school email account set up on your mobile device you must ensure that your device is sufficiently protected from misuse with a lock-screen. This can be with a pin number, pattern, biometric login or, in some cases, facial recognition.

Personal Emails on School Account

Due to the ever increasing volume and sophistication of hoax/fraudulent emails we are all required to be more vigilant than ever before when it comes to checking our school inbox. Because of this, it is highly recommended that we do not use our work email address for any personal use.
Any non-work emails received into our school mailbox, whether solicited or otherwise, makes it much harder to spot those hoax or phishing emails asking you, for example, to log in to your 'Paypal' account.