SINCE 604 AD

# KING'S SCHOOL

## ROCHESTER

# KING'S SCHOOL ROCHESTER
# INFORMATION SECURITY POLICY

| Policy last reviewed on: | 01.09.23 |
|---|---|
| Person/Body reviewing: | DJG/SMT |
| Date of next review (except in the case of relevant legislation): | 01.09.24 |
| Published: | Governors/Staff/Pupils/Website |

# 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 in the School's Employment Manual.  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.

      1.2.2    Information and Records Retention 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 School's data protection policy.

1.4     Any questions or concerns about your obligations under this policy should be referred to the Data Protection Officer (DPO).  Questions and concerns about technical support or for assistance with using the School IT systems should be referred to the IT 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 a 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 rather than blind carbon copy to send emails to multiple recipients.

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 respective Head of School, Bursar or the DPO 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 DPO.  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 DPO and the IT Helpdesk if you become aware of anything which might mean that there has been a security breach.  You must provide your  respective Head of School, Bursar or DPO with all of the information you have.  If you cannot get hold

of your manager or DPO or it is outside of school hours then please use this emergency contact number 07947 739452. 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 individual's privacy more robustly please speak to the DPO.

3.2    From May 2018, the School has been 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 School to identity the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let the DPO 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 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. 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    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 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 DPO.

## 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.  If you are not sure how to do this then speak to the IT Helpdesk.

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 Critical School Personal Data.  For example, safeguarding information should not ordinarily be saved using alumni database software.  If in doubt, speak to the DPO.

6.4    **Hardware and software not provided by the School:** Staff must only download or install software, apps, browser extensions, or services sanctioned by the Director of Digital Strategy.  Staff are allowed to connect private devices (mobile or cabled) using the Kings Wi-Fi network (not the Kings WLAN or Kings Guest unless directed otherwise).

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

6.6 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) 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 IT Helpdesk will protect any portable media device given to you with encryption.

6.7 **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.

## 7 Passwords

7.1 Passwords should be a mix of uppercase and lowercase, numbers and special characters (e.g. #, &, !), should be at least eight characters in length and 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.

7.3 Passwords should be changed every 6 months (the IT Helpdesk will send you a prompt during the February half term and at the beginning of the Academic year to make the change) and your updated password should not be similar to the previous one (for example, do not change your password by just adding a number each time, e.g. orchard1, orchard2, orchard3 etc.).

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

8.1 When sending emails 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 so that names and email address are not visible to other recipients.

8.3 Staff should take particular care when sending any email that contains critical school personal information. Where possible, staff should enable a send delay of 30 seconds in Gmail to allow for the unsending of an accidental email.

8.4 **Encryption:** It is good practice to encrypt attachments to internal and external emails which contain Critical School Personal Data (critical personal data should not be included within the body of the email). For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption then you may need to speak to IT Helpdesk who will explain how to do this. If you need to give someone the "password" to unlock an encrypted 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 @kings-rochester.co.uk 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 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 is only stored in the cabinet in the Principal's study.

| Cabinet | Access |
|---|---|
| Child protection - located in the Principal's office | Only the Principal, the DSL, the Principal's PA and the Safeguarding Administrator have access to this cabinet. |
| Critical Financial information - located in the Bursar's office | Only the Principal, the Bursar and their assistants have access to this cabinet. |
| Health information etc. located in the Medical office | Only the Medical Department staff have access to this cabinet. |

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste sacks which are available through the Bursar's assistant and stored in the locked cupboard in the Accounts office until collected by the School's classified disposal company. 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 DPO. The School uses "follow me" printing which means that you cannot print something out unless 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 School Personal Data. Please see paragraph 9.2 above for details of where Critical School 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 the IT Helpdesk to put in on an encrypted memory stick or arrange for it to be sent by courier.

## 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.

10.3 **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 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 **Using School laptops, phones, cameras and other devices:** If you need to book out a School device then seek advice from the IT Helpdesk.

10.7 Under normal circumstances critical School Personal Data should not be taken off the site in paper format. However, there may be occasions when it is necessary to take critical personal data off site (i.e. School visits and sports fixtures) and permission should be obtained from your respective Head of School or the Bursar and the information should be kept secure as outlined above.

## 11 Using personal devices for School work

11.1 **Accessing School Resources:** Staff are permitted to access Google Workspace, which includes Gmail, Google Drives, and Shared Drives, and other services as directed using a range of devices such as laptops, Chromebooks, iPads, personal devices, and mobile phones. Google Workspace is password-protected, and staff must adhere strictly to the protocol of not sharing login details with anyone. When viewing personal or confidential information, privacy must be maintained at all times.

11.2 **Storage of School Documents:** Documents must not be copied to personal device storage. All modifications to school-related documents should be made directly within the appropriate Google Drive or Shared Drive folder.

11.3 **Security Protocols:** Appropriate security measures must be implemented, encompassing the activation of firewalls and updated anti-virus software. All software or operating systems on personal devices must be maintained up-to-date.

11.4 **Password Management:** Default passwords on personal devices used for school purposes must be altered immediately. For guidelines on generating strong passwords, please refer to section 7 of this policy document.

11.5 Data Protection: Transmission or storage of documents containing Personal Data (including photographs and videos) to personal devices is generally not permitted unless explicit permission has been granted by the Data Protection Officer (DPO). This is to ensure that such data remains within the protective framework of the School's security systems. Erasing such data from personal devices can be complicated and is often not completely effective.

11.6 **Friends and family:** Family and Friends: Measures must be enacted to prevent unauthorized access to school-related information by others who might use your personal device. Logging out of school accounts and restarting the device after work is completed are required steps. If there is uncertainty about the security settings on the device, consultation with the IT Helpdesk is strongly advised.

11.7 Termination of Use: If a staff member ceases to use a personal device for school-related work due to any of the following reasons:

11.7.1 A decision to stop using the device for school purposes,

11.7.2 Withdrawal of the School's permission to use the device, or

11.7.3 Impending departure from the School,

all school-related documents and software applications must be removed from the device. If remote removal is not possible, the device must be submitted to the IT Helpdesk for data wiping and software uninstallation. Full cooperation with the IT Helpdesk during this process is mandatory.

## 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.