

Information Security Policy

Duke of Kent School

September 2024

1 Introduction

- 1.1 Information security is about what you and the School need to do to keep **Personal Data** secure. This is the most important area of data protection to get right. Most data protection fines have come about because of information security breaches.
- 1.2 This policy must be read alongside the School's Data Protection Policy: Practical Guidance for Staff which gives an overview of your, and the School's, obligations around data protection. The Policy can be found in the Employment Manual on the Staff Google Drive. In addition, you must also read the following which are relevant to data protection:
 - 1.2.1 IT acceptable use policy for staff;
 - 1.2.2 Guidance for Staff on the Use of Photo and Videos; and
 - 1.2.3 Information and Records Retention Policy (if relevant to your role).
- 1.3 This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, peripatetic staff, work experience / gap year / placement students and volunteers.
- 1.4 Data protection is the responsibility of everyone in the School, and it is important that you read and understand the relevant policies so that you know what you must do day-to-day, but also what to do when something goes wrong.
- 1.5 Any questions or concerns about your obligations under this policy must be referred to the Data Protection Lead. Questions and concerns about technical support, or for assistance with using the School IT systems, must be referred to the Network Manager.

2 Be aware and report concerns

- 2.1 You must keep School Personal Data confidential and take steps to make sure that it is not seen by anyone unless they are entitled to see it. In this policy, School Personal Data means any Personal Data relating to the School such as personal data about staff, pupils and parents.
- 2.2 Information security breaches can happen in a number of different ways. Examples include:
 - 2.2.1 opening a suspicious attachment in an email;
 - 2.2.2 not being able to access a document because the password has been forgotten;
 - 2.2.3 an unencrypted laptop stolen after being left on a train;
 - 2.2.4 Personal Data held to ransom following a website hack;
 - 2.2.5 inadvertently displaying information (for example a confidential email) via a screen share or interactive whiteboard;
 - 2.2.6 sending a confidential email to the wrong recipient; and
 - 2.2.7 leaving documents containing Personal Data on a doorstep.
- 2.3 These should give you a good idea of the sorts of things that 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 and the Data Protection Lead if you have any ideas or suggestions about improving practices. One option is to have team specific checklists to help ensure data protection compliance. Think about other teams as well, another example of something that must be reported is where you become aware that a particular department has developed a habit of leaving confidential documents in unlocked classrooms.

- 2.4 You must immediately tell the Data Protection Lead and the Network Manager if you become aware of anything that might mean that is a risk to School Personal Data, if you suspect a security incident or data breach or if you become aware of a practice that weakens the School's defences in relation to the protection of Personal Data. The sooner you tell someone the easier it is for the School to respond and put things right.
- 2.5 If you cannot get hold of the Data Protection Lead or it is outside of school hours, then please use this emergency contact number 07984649931 (Data protection Lead).
- 2.6 You must report even if you are not certain that something has gone wrong. For example, if you accidentally send an email to the wrong recipient, or you cannot find some papers which contain Personal Data. You must report this even if there is no evidence that they have been accessed or stolen. You must report anything which puts Personal Data at risk, for example, if Personal Data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen.
- 2.7 The School must report certain data breaches to the Information Commissioner's Office (the data protection regulator) within 72 hours, and also let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately. You must report even if you are not directly involved.
- 2.8 Pupils can also pose a risk to the School, particularly those pupils who have a good understanding of IT. Many schools have had their computer systems compromised by pupils. If you have any suspicions, please raise them as explained above.

3 Thinking about privacy day-to-day

- 3.1 You should be thinking about data protection and privacy whenever you are handling Personal Data. Personal Data is virtually anything recorded about someone, even something as simple as a person's address or hobbies. Our Data Protection Policy: Practical Guidance for Staff includes more information on what Personal Data is.
- 3.2 If you have any suggestions for how the School could improve its data protection / information security practices or protect individual's privacy more robustly, please speak to the Data Protection Lead.
- 3.3 In some situations, the School is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. These assessments are known as Data Protection Impact Assessments. For example, when we introduce new technology which represents a particular risk to privacy.
- 3.4 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 or would be helpful, please let the Data Protection Lead know.

4 **Critical School Personal Data**

- 4.1 Data protection is about protecting 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: Practical Guidance for Staff.
- 4.2 Critical School Personal Data is information about:
- 4.2.1 child protection or safeguarding matters;
 - 4.2.2 someone's special educational needs;
 - 4.2.3 a serious allegation made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved);
 - 4.2.4 financial information (for example, a parent's bank details or a staff member's salary);
 - 4.2.5 an individual's racial or ethnic origin;
 - 4.2.6 an individual's political opinions;
 - 4.2.7 someone's religious or philosophical beliefs;
 - 4.2.8 trade union membership;
 - 4.2.9 someone's physical or mental health or condition. This includes information about the provision of health care which reveals information about their health status;
 - 4.2.10 sex life or sexual orientation;
 - 4.2.11 genetic information;
 - 4.2.12 actual or alleged criminal activity or the absence of criminal convictions (e.g. Disclosure and Barring Service checks); and
 - 4.2.13 biometric information that uniquely identifies someone (e.g. fingerprints used for allowing access to buildings).
- 4.3 Staff need to be extra careful when handling Critical School Personal Data.
- 4.4 If you are sharing Critical School Personal Data, for example via email, then you must mark the message as SENSITIVE / HIGHLY SENSITIVE before sending.

5 **Minimising the amount of Personal Data that we hold**

- 5.1 Restricting the amount of Personal Data, we hold to what is needed helps keep Personal Data safe, but you must never delete Personal Data unless you are sure you are allowed to do so.
- 5.2 If you would like guidance on when to delete certain types of information, please speak to the Data Protection Lead.

6 **Using computers and IT**

- 6.1 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.

- 6.2 **Lock computer screens:** your computer screen must 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 the Network Manager. The School's computers are configured to automatically lock if not used for 3 minutes for Support/Office staff pc's and 10 minutes for teacher's pc's and Chromebooks.
- 6.3 **Close programmes and windows when not in use:** make sure you close any programmes or windows when not being used or where someone else may be able to see your screen. You must also ensure your notifications and pop-up alerts are switched off. For example, when screen sharing with pupils as part of a lesson or when using an interactive whiteboard. Emails and other programmes that contain personal data must not be accessed while screen sharing or using an interactive whiteboard.
- 6.4 **Be careful when looking at confidential emails and documents:** don't view confidential emails or documents whilst teaching, whilst pupils are around, or if there is a risk that the contents will be seen by someone unauthorised.
- 6.5 **Be familiar with the School's IT:** you must 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 how to deal with any risks. For example:
- 6.5.1 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 accidentally upload anything more sensitive;
 - 6.5.2 make sure that you know how to properly use any security features. For example, some software will allow you to redact documents. Make sure that you can use this software correctly so that the recipient of the document cannot "undo" the redactions; and
 - 6.5.3 you need to be extra careful where you store information containing Critical School Personal Data. For example, safeguarding and child protection information must not be saved anywhere but on the "My Concern" platform which is a specific safeguarding software programme available only to the Head, DSL and Deputy DSL's. If in doubt, speak to the Data Protection Lead.
- 6.6 **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 Network Manager. 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 from the Network Manager.
- 6.7 **Private cloud storage:** you must not use private cloud storage or file sharing accounts to store or share School documents or anything containing School Personal Data. You must only use cloud storage provided by the School.
- 6.8 **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 Network Manager will protect any portable media device given to you with encryption. You must not plug in or connect anything not provided by the School to School computers or other equipment, even if it looks harmless. This is because something that looks innocuous such as a USB charging cable can be harmful.

- 6.9 **School IT equipment:** if you are given School IT equipment to use (this includes laptops, printers, phones, cameras, USB drives and DVDs), this will be recorded on the School's IT equipment asset register by the Network Manager. School IT equipment must always be returned to the Network Manager even if you think that it is broken and will no longer work and the asset register updated accordingly. Cameras are usually held by the Head of Art who will also record the issue and return of this equipment.
- 6.10 **Where to store electronic documents and information:** you must ensure that you only save or store electronic information and documents in the correct location on the School's systems as follows:
- 6.10.1 Google Workspace (cloud service) for pupil's work/homework and Shared Google Drives for Staff. Google mail for all staff.
 - 6.10.2 ISAMS (The School's cloud base Management Information System) for pupil information. Access to all teaching and office based staff and overseen by the Director of Teaching and Studies.
 - 6.10.3 Oasis platform for school financial information including fee details for parents and payroll details for staff, operated by the Finance Office team.
 - 6.10.4 Paper (cloud based HR system) for staff operated by HR staff.
 - 6.10.5 Photo Store network drive for pupil and school photographs.
 - 6.10.6 Website (cloud based service) for school information including a secure portal for parents with log in credentials.
 - 6.10.7 Various network drives for support staff for operational documentation including policies.

7 Passwords

- 7.1 Passwords must be as long as possible and difficult to guess. The longer a password the more difficult it is to hack.
- 7.2 Create a password using three random words with special characters and numbers (e.g. *82@GiraffeSparklingBlue*) but this is not mandatory.
- 7.3 Make sure that the words are unrelated to each other. The advantage of three well-chosen random words is that they can be easy to remember but not easy to guess.
- 7.4 Make sure your password is memorable but don't choose words or numbers that are linked to you like the names of your family members or words related to the School. Do not choose a password which is so complex that it's difficult to remember without writing it down.
- 7.5 You must not use a password which you use for another account.
- 7.5.1 For example, you must not use your password for your private email address or online shopping account for any school account.
 - 7.5.2 This is because if your personal account is compromised this presents a risk of access to the School's systems as well. Neither must you use your work email address for personal things online (e.g. online shopping).

- 7.6 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 must not be written down.

If your email address has been compromised, please speak to the Network Manager as a matter of urgency.

- 7.7 Sometimes a computer or web browser will allow you to save the password so that you do not need to type it in again next time. You must make sure this does not happen, for example, by declining any request from the browser to save the password.

8 **Cyber-attacks and related risks**

- 8.1 Schools are frequently targeted by attackers looking to take advantage of vulnerabilities in school systems and processes. Sometimes, such attacks will look to exploit technical weaknesses, whilst on other occasions attacks will focus on the human element.

- 8.2 For example, an attacker might encourage someone to click on a link in an email by making the email appear as if it has come from a trusted source such as a colleague. This is commonly known as a phishing attack. Phishing attacks are usually done by email or text but can also be via social media. You can reduce the likelihood of a phishing attack by thinking about what information you (and others) post about you, and by reviewing your privacy settings on your social media accounts.

- 8.3 Hackers will sometimes carry out research to help make their communications appear genuine (e.g. research what job you have at the School). They might even have discovered one of your passwords used outside of the School through another cyber-attack and mention this.

- 8.4 For example, a phishing email might appear to be from the School's IT team and state that you must click on a link to reset your password immediately or you will lose all of your emails. If you click on the link it would take you a page that looks genuine and asks you to input your current password and create a new one. The hacker then has your password and can use this to access the School's systems.

- 8.5 The following are examples of the types of things to look out for in emails and text messages:

8.5.1 a request for information, especially financial information;

8.5.2 a request to click a link or open an attachment;

8.5.3 the sender telling you that it is urgent or pressuring you to act;

8.5.4 the sender appears as though they have authority or power;

8.5.5 poor language or spelling;

8.5.6 a payment request from a supplier using an email address that is not their usual email address; or

8.5.7 unusual sender details or an email address that doesn't look quite right. Often someone may try to pretend that they are emailing you from a school email address. For example, the email address after the @ symbol might contain the name of your

school but the spelling is incorrect, or the suffix at the end of the email might be different (e.g. .org rather than org.uk or vice versa).

- 8.6 Alternatively, an email or text may appear as if it's from someone who is providing technical support. For example, it might ask for your password or other credentials. Never share your password with anyone. IT will never ask for this.
- 8.7 If you find that you cannot access a particular programme, system or set of data, you must contact the Network Manager immediately. Whilst this could just be a technical fault, it could be evidence that someone has been able to gain access to the School's systems.
- 8.8 Sometimes the attacker may be someone known to the School, such as a parent or pupil. For example, following an acrimonious divorce a parent may set up an email address using the other parent's name in order to try to trick the School into sending them information concerning the other parent.
- 8.9 If you are asked to provide Personal Data over the phone, make sure that the request is genuine. For example, by calling the individual back using the number you have on the system. In most cases, this must be done even if the person says that they are in a position of authority, such as the police.
- 8.10 Sometimes hackers create fake links to advertisements which are displayed on websites. When you click on the link or advert a malicious programme is downloaded.
- 8.11 You must also be on your guard if anyone asks you to change Personal Data held by the School. Compromising the accuracy of Personal Data is also a breach, even if it is accidental.
- 8.12 You must be familiar with the School's normal policies and procedures relevant to your role (e.g. around the payment of invoices) so that you can more easily spot an unusual request.
- 8.13 Hackers will sometimes use information about people found online to increase the likelihood that their attack will succeed. For example, if they know that you have access to financial information they might use this to target you. You must be careful about what you publish online regarding your job.
- 8.14 If you fall victim to any form of scam or attack, you **MUST** report this immediately so that the School can take the necessary steps to minimise the impact of the action, and report where necessary. Please see section 2 above. Every successful cyber-attack that goes unreported, with no investigation or information sharing, makes other attacks and repeat attacks more likely.
- 8.15 If you receive a suspicious message, you must inform the Network Manager immediately rather than simply ignoring the message.

9 Email and telephone (including text messaging and messaging apps)

- 9.1 You must take care to make sure that the recipients are correct. Getting an email address or telephone number wrong is one of the most common causes of a breach.
- 9.2 Double check email attachments before sending by opening them after you have attached them to the email. Check that documents don't have any "hidden" data. For example, spreadsheets that have hidden rows or columns.
- 9.3 **Emails to multiple recipients:** Multiple recipient emails sent from the School's Google mail system do not reveal individual email addresses to recipients. These types of email will

usually be sent by the Network manager or Head's PA and will be directed to members of the school community only. A similar arrangement to send emails to multiple recipients can be undertaken through the School's MIS (ISAMS) although this system will only send individual emails to each recipient. Emails from the school's MIS would usually originate from teaching or office staff.

- 9.4 **Forwarding email chains:** always check the entire email chain before forwarding on.
- 9.5 **Encryption:** remember to encrypt internal and external emails that contain Critical School Personal Data. For example, encryption must be used when sending details of a safeguarding incident to social services. To use encryption then you need to speak to the Network Manager 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 must be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password.
- 9.6 **Non-school email addresses:** you must not use a non-school email address for sending or receiving School Personal Data. You must only use a school email address, i.e. one that ends in @dokschoo.org. Please note that this rule applies to governors as well. Please speak to the Network Manager if you require an email account to be set up for you.
- 9.7 **Messaging apps:** you must not use messaging apps (e.g. WhatsApp) for sharing School Personal Data unless you have been given permission by the Data Protection Lead.

10 Paper files

- 10.1 **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. If you take Personal Data with you to a meeting, make sure that you collect all of your papers when you leave.
- 10.2 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 held in paper format must not be stored in any other location, for example, child protection information must only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room. The cabinets are located around the School as follows:

Cabinet	Access
Child protection - located in the DSL's office	Key access to cabinet which is available to the DSL and Deputy DSL's only.
Financial information - located in the Finance office	The Finance Office is locked when not attended with key access only by Head of Finance and Assistant Head of Finance. Spare key is located in the key safe at top of cellar stairs, only accessible to the Head, Head of Operations, Network Manager and Head of Maintenance. There is also a store next to the medical Room where financial and HR records are stored. This store is locked and only accessible to Finance and Bursary staff as above.

Health information documents located in the Medical Room	Medical Room locked when not attended by School nurses who have key access, with a master key available to Head of Operations and office staff who cover the medical room after 3.30pm term time. Health records are held in lockable fire proof cabinets with keys held by School nurses.
Staff HR files located in the Bursar's office	HR files are stored in the Bursary in fire proof filing cabinets which are duly locked with keys available to Bursary staff only.
Pupil records (Registration/Acceptance forms and general correspondence) located in the Main School Office.	All pupil files held in the School Office in fire proof lockable cabinets. Head's PA and Registrar are sole key holders. Office locked when not in use.

- 10.3 **Disposal:** paper records containing Personal Data must be disposed of securely by shredding. Shredders are located in the Staff Room and in the Bursary, supplemented by on site shredding by a secure mobile unit when required – fully certificated. Personal Data must never be placed in the general waste.
- 10.4 **Printing:** you must 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 Data Protection Lead.
- 10.5 **Put papers away:** you must 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 must not be used to store documents containing Critical School Personal Data. Please see paragraph 10.2 above for details of where Critical School Personal Data must be kept.
- 10.6 **Displays:** be aware of what Personal Data is on display when the classroom is being used for lessons. For example, would it be possible for pupils to read information that is on your desk while you are teaching? Additionally, if any photographs or videos are being taken on the school premises, you must ensure that there is no Personal Data in the background (e.g. on school displays) that could be accidentally captured and made public by the photograph or video.
- 10.7 **Post:** you also need to be extra careful when sending items in the post. Confidential materials, including anything which contains Critical School Personal Data, must not be sent using standard post. If you need to send something in the post that is confidential, consider asking the Network Manager to put in on an encrypted memory stick or arrange for it to be sent by secure courier.
- 11 **Working off site (e.g. school trips and homeworking)**
- 11.1 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 appropriate safeguards are in place.

- 11.2 For School trips, the trip organiser is responsible for deciding what information needs to be taken and who will look after it. You must make sure that any Personal Data taken off site is returned to the School.
- 11.3 If you are allowed to work from home, then check with the Data Protection Lead what additional arrangements are in place in relation to paper records and accessing information electronically. This might involve installing software on your home computer or smartphone, please see section 12 below. You must never email anything containing School Personal Data either from or to a non-school email address.
- 11.4 Not all staff are allowed to work from home. If in doubt, speak to the Data Protection Lead.
- 11.5 **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 them 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 must only take the information about the eight pupils.
- 11.6 **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). If working on a laptop on a train, you must 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. A privacy screen may help.
- 11.7 **Return the documents:** make sure that documents are returned to the School. For example, if you print off some information for a school trip, make sure the print out is returned once the trip has finished.
- 11.8 **Paper records:** if you need to take hard copy (i.e. paper) records off school site then you must make sure that they are kept secure. For example:
- 11.8.1 documents must be kept in a locked case. They must also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);
 - 11.8.2 if travelling by train you must keep the documents with you at all times and they must not be stored in luggage racks;
 - 11.8.3 if travelling by car, you must keep the documents out of sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights; and
 - 11.8.4 if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you must 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 sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you (please see paragraph 11.5 above).
- 11.9 **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 4G/5G.
- 11.10 **Using School laptops, phones, cameras and other devices:** if you need to book out a School device then please liaise with the Network Manager. Please see 6.8 and 6.9 above for more information.

- 11.11 Critical School Personal Data must 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 11.5 above). Other than School trips, you must obtain authorisation from the Data Protection Lead.
- 11.12 **When you leave us:** when you leave the School (e.g. to start a new job or to retire) you must return any Personal Data (and documents containing personal data) to the Data Protection Lead or to your Line Manager before the end of your last day (or earlier if requested). For example, if you have been given permission to keep papers at home you will need to make sure that these are returned. Please also see 12.12 below in relation to electronic devices used for School work.

12 Using personal devices for School work

- 12.1 You may only use your personal device (such as your laptop or smartphone) for School work if you have been given permission by the Data Protection Lead. Please also see paragraph 6.9 above.
- 12.2 Even if you have been given permission to do so, then before using your own device for School work you must speak to the Network Manager so that they can configure your device.
- 12.3 **Using your own laptop or PC:** if you use your computer for School work then you must use the remote access software provided by the School known as Team Viewer. Using Team Viewer means that Personal Data is accessed through the School's own network which is far more secure and significantly reduces the risk of a security breach. Currently, the Network Manager is the only person who has remote access to the internal School network via Team Viewer and this is to ensure that the integrity of the network is maintained outside of school hours in case of need.
- 12.4 **Using your own smartphone or handheld:** Personal devices should not be used for School work unless in exceptional circumstances you have made arrangements with the Network Manager and suitable software, if applicable, has been loaded onto your device to keep personal data secure and separate from private files. However, it is acknowledged that there may be occasions when you may need to access your school email account via your personal device and in these circumstances, the following guidance should be followed;
- 12.4.1 Your personal device must have a screen lock in place which can only be unlocked by pin, password, pattern, finger print or face ID. (see 12.7 below).
- 12.4.2 Your personal device should not be used on School premises.
- 12.4.3 Your school email account must be accessed via a browser and not configured within an App or email client.
- 12.4.4 Your log on credentials for the email account must not be saved on the device.
- 12.5 **Appropriate security measures** must always be taken. This includes making sure that the firewall on your device is enabled and using anti-virus software and malware protection. Any software or operating system on your device must be kept up to date by promptly installing updates when they become available. You must make sure that you are using an operating system which is still supported (so you must not use an old version of Windows, such as Windows 7, for example).

- 12.6 **Downloading apps and software:** you must take care when downloading apps or software onto your personal device if it is used for School work. This is the case even if you are using remote access software. Hackers can exploit vulnerabilities in your personal device to access School Personal Data. Please only download apps from official app stores like the Apple App Store and Google Play. If you have any questions, please speak to the Network Manager.
- 12.7 **Screen lock and password:** you must have a screen lock on any mobile device used to access School Personal Data (e.g. a passcode or fingerprint). Any computer (e.g. laptop) used for School work must be protected with a strong password (see section 7 above).
- 12.8 **Default passwords:** if you use a device for work which came with a default password then this password must be changed immediately. You must also change the default password on any account used for work reasons even if you are not using it to share Personal Data. Please see section 7 above for guidance on choosing a strong password.
- 12.9 **Sending or saving documents to your personal device:** documents containing Personal Data (including photos and videos) must not be sent to or saved to personal devices, unless you have been given permission by the Network Manager.
- 12.9.1 This is because anything you save to your computer, tablet or mobile phone will not be protected by the School's security systems.
- 12.9.2 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.
- 12.10 **Friends and family:** you must not share School Personal Data with your friends and family or allow them to access or see School Personal Data. For example, you must not share the login details with others and you must log out of your account once you have finished working and restart 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 Network Manager. Disclosing School Personal Data to your friends and family is a data breach, and if you do so knowingly or recklessly, you might be committing a criminal offence. The School is likely to consider breaches of confidentiality as a disciplinary matter.
- 12.11 **Social media:** You must never upload or publish School Personal Data using your personal social media account, even if your account is set to private. For example, you must not upload photos of pupils under any circumstances.
- 12.12 **When you stop using your device for School work:** if you stop using your device for School work, for example:
- 12.12.1 if you decide that you do not wish to use your device for School work; or
- 12.12.2 if the School withdraws permission for you to use your device; or
- 12.12.3 if you are about to leave the School;
- then you must ensure that all School documents (including School emails), and any software applications provided by us for School purposes, are removed from the device.

If this cannot be achieved remotely, you must submit the device to the Network Manager for wiping and software removal. You must provide all necessary co-operation and assistance to the Network Manager in relation to this process.

- 12.13 **Disposal:** if you need to dispose of IT equipment, you must make sure no personal data is left on any of the devices before you dispose of them. You must check with the Network Manager to ensure that this is done correctly.

13 **Breach of this policy**

- 13.1 Any breach of this policy will be taken seriously and may result in disciplinary action.
- 13.2 A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the School (or procures its disclosure to another person) without proper authority might also be committing a criminal offence and gross misconduct. This could result in summary dismissal. Further information on this and on other offences can be found in the School's Data Protection Policy: Practical Guidance for Staff.
- 13.3 Employees only: This policy does not form part of your contract of employment and may be amended by the School at any time.
- 13.4 We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

Information Security Top Tips

1. Speak to the Data Protection Lead / Privacy Officer if you have any concerns, questions or suspicions.
2. If you have any questions about the School's IT systems speak to the Network Manager.
3. If it's an emergency (e.g. you suspect a data breach) call the Data Protection Lead on 07984649931.
4. If you need to dispose of any School Personal Data, this must be done securely (e.g. use the Shredders in the Staff Room and Bursary).
5. Your passwords must be strong and unique (please see section 7 of the Information Security Policy for more information).
6. School Personal Data must never be sent to a non-school email account that you use.
7. Be on your guard for suspicious emails, texts and phone calls. Never click on a link, open an attachment or provide information if you have any doubts - check with the network Manager first. See section 8 of the Information Security Policy.
8. Be extra careful to keep Personal Data secure when working away from the School site. For example, only take the minimum amount of Personal Data with you. See section 11 of the Information Security Policy.
9. You must only use a personal device (e.g. phone, tablet, laptop) for school work if this has been approved by the data protection Lead and you understand how to access School Personal Data securely. See section 12 of the Information Security Policy.
10. Personal Data must be sent securely. Never send anything confidential or sensitive by normal post. Speak to the Network Manager if you need to send something electronic securely.

These are some key points to remember. You must still read and follow the Information Security Policy, which goes into a lot more detail.