Information Security Policy

Independent Day and Boarding School for Boys and Girls



Ellesmere

Veale Wasbrough Vizards

1 Introduction

1.1 Information security is about what you and the College 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 College's data protection policy which gives an overview of your and the College's obligations around data protection. The College's data protection policy can be found here www.ellesmere.com In addition to the data protection policy, you should also read the following which are relevant to data protection:

1.2.1 the College's privacy notices for staff, pupils and parents; and

1.2.2 IT acceptable use policy for staff.

1.3 This policy applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see the College's data protection policy.

1.4 Any questions or concerns about your obligations under this policy should be referred to the Director of Finance who is the Data Protection Lead. Questions and concerns about technical support or for assistance with using the College IT systems should be referred to the IT Department.

2 Be aware

2.1 Information security breaches can happen in a number of different ways. Examples of breaches which have been reported in the news include:

2.1.1 an unencrypted laptop stolen after being left on a train;

2.1.2 Personal Data taken after website was hacked;

2.1.3 sending a confidential email to the wrong recipient; 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 line manager and the Director of Finance 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 Director of Finance. 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 Director of Finance and the IT Department if you become aware of anything which might mean that there has been a security breach. You must provide your line manager or the Director of Finance with all of the information you have. If you cannot get hold of your line manager or the Director of Finance or it is outside of school hours then please contact another member of SMT. All of the following are examples of a security breach:

2.4.1 you accidentally 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 Staff must remain vigilant to cyber security threats including phishing emails, malicious attachments, social engineering attempts, ransomware attacks and fraudulent requests for information. Suspicious communications must be reported immediately to the IT Department and Director of Finance.

2.6 In certain situations, the College must report a personal data breach to the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of the breach. In some circumstances affected individuals must also be informed. Prompt reporting by staff is therefore essential.

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 College could protect individual's privacy more robustly please speak to the Director of Finance.

3.2 From May 2018, the College 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 College 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 Director of Finance know.

4 Critical 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 Personal Data** in this policy and in the data protection policy. Critical 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. fingerprints used for controlling access to a building).

4.2 Staff need to be extra careful when handling Critical 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 Director of Finance.

5.2 Personal data must only be retained for as long as necessary and in accordance with the College's Records Retention Schedule. Staff must ensure records are securely disposed of when retention periods have expired.

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 College'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 and the "L" key simultaneously. If you are not sure how to do this then speak to IT. The College's computers are configured to automatically lock if not used for 15 minutes.

6.3 **Be familiar with the College'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 College 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 Personal Data. For example, safeguarding information should not ordinarily be saved using alumni database software. If in doubt, speak to the Director of Finance.

6.4 **Hardware and software not provided by the College:** Staff must not use, download or install any software, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the College Core network without permission. **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share College documents.

6.5 College information must only be stored within College-approved systems and cloud services. Staff must not store College information in personal online storage locations or applications. Approved systems include College-managed Microsoft 365 services and other systems authorised by the IT Department.

Where Multi-Factor Authentication (MFA) is available it must be enabled and used for College systems and accounts. Staff must not bypass or disable MFA controls.

6.6 **Disposal of College IT equipment:** College 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 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 Passwords must be strong and unique. Passwords should contain at least sixteen characters for staff, 12 characters for senior school and 8 characters for Lower School include a combination of words, letters, numbers and symbols where required by the system.

7.4 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.

7.5 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.

7.6 Passwords should be changed immediately if compromise is suspected. Routine password changes are every six months.

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:** When sending emails to multiple recipients, staff should always use SIMS InTouch if for parents or others who are on SIMS. Otherwise lists should be checked for erroneous recipients.

8.3 If the email or fax contains Critical 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 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 Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To encrypt a single message:

1. In the message that you are composing, on the Options tab, in the More Options group, click the dialog box launcher in the lower-right corner.

2. Click Security Settings, and then select the Encrypt message contents and attachments check box.
3. Compose your message, and then click Send.

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 Staff must exercise particular caution before opening links, attachments or files received from unknown or unexpected sources. Any suspected phishing email must be reported to the IT Department immediately and must not be forwarded outside approved reporting procedures.

8.6 **Private email addresses:** You must not use a private email address for College related work. You must only use your @ellesmere.com address. Please note that this rule applies to Governors as well. Please speak to the IT Department if you require an email account to be set up for you.

9 Paper files

9.6 **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.

9.7 If the papers contain Critical 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 the cabinet in the Deputy Head Pastoral (DHP) room. These cabinets used by the College are kept in a secure location. They are also too heavy to move to minimise the risk of theft. The cabinets are located around the College as follows:

Cabinet	**Access**
Child protection – located in the DHP's office	Only DHP and DHA have access to the old paper files. CPOMS holds the electronic safeguarding records. Access is restricted to trained Designated Safeguarding Leads and authorised safeguarding personnel only. Access permissions are reviewed regularly.
Financial information - located in the Director of Finance's office	Director of Finance and the Accountant have access to the files.
Health information - located in the sickbay	All School Nurses have access to the files.
Main Pupil files in the Head's Secretary office	Only the Head or his deputies and the Head's Secretary can allow access.
Staff files (Teachers)	Only the Head or his deputies and the Head's Secretary can allow access.

Staff files (Non-Teaching	Only the Head, his deputy, Estates Manager and Compliance Secretary have access.

9.8 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bags or shredding them Personal Data should never be placed in the general waste.

9.9 **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 Director of Finance. Make sure you are aware which printer your documents will print to.

9.10 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed.

9.11 **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.

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

10.1 Staff might need to take Personal Data off the College site for various reasons, for example because they are working from home or supervising a trip. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

10.2 For 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 College.

10.3 If you are allowed to work from home then check with the Director of Finance what additional arrangements are in place.

10.4 When accessing College systems remotely, staff must use College-approved secure connections and authentication methods. Public or unsecured Wi-Fi networks should not be used for accessing confidential information unless protected by approved security controls.

10.5 **Take the minimum with you:** When working away from the College 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.

10.6 **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). 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.

10.7 **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 10.4 above).

10.8 **Using College laptops, phones, cameras and other devices:** If you need to book out a College device then use the College booking system.

10.9 Critical 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 trips (see 10.4 above).

11 Using personal devices for College work

11.1 You may use your personal device (such as your laptop or smartphone) for College work.

11.2 Before using your own device for College work you may need to speak to your IT team so that they can configure your device. Any personal device used for College business must be protected by a password, PIN, biometric authentication or equivalent security control and configured to lock automatically when not in use.

11.3 **Using your own PC or Laptop:** If you use your laptop or PC for College work then you must use the remote access software provided by the College known as RD client in all cases. Using RD client means that Personal Data is accessed through the College's own network which is far more secure and significantly reduces the risk of a security breach. All links to the remote desktop are on the College website via the Remote Access link.

11.4 **Appropriate security measures** should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date. Where technically possible, personal devices used for College business should support remote wiping of College data in the event of loss, theft or compromise.

11.5 **Default passwords**: If you use a personal device for College 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.

11.6 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should not normally be sent to or saved to personal devices, unless you have been given permission by the IT Department. This is because anything you save to your computer, tablet or mobile phone will not be protected by the College'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 College 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.

11.7 **Friends and family:** You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything College 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 College related documents and information – if you are unsure about this then please speak to the IT Department.

11.8 **When you stop using your device for College work:** If you stop using your device for College work, for example:

11.8.1 if you decide that you do not wish to use your device for College work; or

11.8.2 if the College withdraws permission for you to use your device; or

11.8.3 if you are about to leave the College

then, all College documents (including College emails), and any software applications provided by us for College purposes, should be removed from the device.

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

12 Information Classification

Information held by the College should be handled according to its sensitivity and confidentiality.

12.1 Information classified as safeguarding, special educational needs, health information, staff records, disciplinary records, financial information and any special category personal data must be treated as Critical Personal Data.

12.2 Staff must ensure that appropriate technical and organisational measures are applied to protect information according to its classification.

13 Breach of this policy

13.1 All staff are required to complete information security and data protection training as directed by the College. Failure to comply with mandatory training requirements may be treated as a breach of this policy. 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 discloses Personal Data held by the College without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

13.3 This policy does not form part of any employee's contract of employment.

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.

Reviewed by	DHP and IT Manager
Review Frequency	Annually
Authorised by	The Head
Next review Date	October 2027