Cabot
Learning
Federation

Information Security Policy

Date Adopted: 25th May 2018, Cabot Learning Federation
Implementation Date: 25th May 2018

History of most recent Policy changes

Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
23/01/2018	Whole document	Updated from VWV template. Copied into CLF template.	
05/03/2018	Whole document	Updated following review across DP working groups.	
01/05/2018	1.2 4 8.5 10.7	Removed section defining CLF and schools. Changed definitions from “special data” to broader definition of “critical data”. Adjusted wording to account for cases where email accounts are not provided. Updated wording to provide more definition of when a locked case would be required.	Review by VWV

Contents

1 Introduction

1.1 Information security is about what you and the Cabot Learning Federation (the **CLF**) 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 CLF's data protection policy which gives an overview of your and the CLF's obligations around data protection. The CLF's data protection policy can be found in the CLF Employment Manual and is also available on the CLF staff intranet website, CLiF. In addition to the data protection policy, you should also read the following which are relevant to data protection:

(a) the CLF's privacy notices for staff, pupils and parents; and

(b) IT acceptable use policy for staff.

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

1.4 The Data Protection Officer is responsible for helping you to comply with the CLF's obligations in relation to data protection. To facilitate access to matters relating to data protection each academy and central team department has a designated Data Protection Lead. The Data Protection Officer works closely with the CLF Corporate Services team in relation to some data protection functions. Together the Data Protection Officer, Corporate Services team and Data Protection Leads are referred to as the **Data Protection Team**. All queries concerning data protection matters should be raised with an appropriate member of the Data Protection Team, this will often be the Data Protection Lead in the first instance.

1.5 Questions and concerns about technical support or for assistance with using the CLF's IT systems should be referred to the CLF ICT Service team.

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:

(a) an unencrypted laptop stolen after being left on a train;

(b) Personal Data taken after website was hacked;

(c) sending a confidential email to the wrong recipient;

(d) leaving confidential documents containing Personal Data on a doorstep;

(e) using carbon copy (CC) rather than blind carbon copy (BCC) 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 manager, or the Data Protection Team 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 Data Protection Team. 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 Data Protection Team or the CLF ICT Service Team if you become aware of anything which might mean that there has been a security breach. You must provide the team with all of the information you have.

2.5 All of the following are examples of a security breach:

(a) you accidently send an email to the wrong recipient;

(b) you cannot find some papers which contain Personal Data; or

(c) 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.

2.6 In certain situations the CLF 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 CLF could protect individual's privacy more robustly please speak to the Data Protection Team .

3.2 From May 2018, the CLF is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a risk to individual's privacy or where Personal Data is used on a large scale, such as CCTV.

3.3 These assessments should help the CLF 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 Data Protection Team 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:

(a) information concerning child protection matters;

(b) information about serious or confidential medical conditions and information about special educational needs;

(c) 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);

(d) financial information (for example about parents and staff);

(e) information about an individual's racial or ethnic origin; and

(f) political opinions;

(g) religious beliefs or other beliefs of a similar nature;

(h) trade union membership;

(i) physical or mental health or condition;

(j) genetic information;

(k) sexual life;

(l) information relating to actual or alleged criminal activity; and

(m) biometric information (e.g. a pupil's fingerprints following a criminal investigation).

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 refer to the data retention policy or speak to the Data Protection Team.

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 CLF'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 the CLF ICT Service team. The CLF's computers are configured to automatically lock if not used for 5 minutes. In some cases this is extended to support learning. In these circumstances staff much ensure workstations are locked when leaving the computer unattended.

6.3 **Be familiar with the CLF'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:

(a) 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;

(b) make sure that you know how to properly use any security features contained in CLF 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

(c) you need to be extra careful where you store information containing Critical Personal Data. For example, safeguarding information should not be saved on a shared computer drive accessible to all staff. If in doubt, speak to Data Protection Team.

6.4 Specific guidance on the information security requirements of the different programmes that the CLF uses can be found in section 13 of this policy.

6.5 **Hardware and software not provided by the CLF:** Staff must not use, download or install any software, app, programme, or service without permission from the CLF ICT Service team. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the CLF IT systems without permission, unless such connectivity is provided and advertised as either "Guest" or "Bring Your Own Device/(BYOD)".

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

6.7 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed **for the storage of Personal Information** unless those devices have been approved by the CLF ICT Service Team and you have received training on how to use those devices securely. For more information about acquiring and encrypting a portable media device speak with the CLF ICT Service team.

6.8 **Disposal of CLF IT equipment:** CLF IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the CLF ICT Service Team 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. If you need help creating and remembering secure passwords review the information available on CLiF or speak with a member of CLF ICT Service team.

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.

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 email to multiple recipients liaise with the CLF ICT Service team to ascertain the safe methods available for doing so. In the case where there are no specific systems to support emailing multiple recipients you must:

8.2.1 always enter the recipients email address in the blind carbon copy (BCC) address box and,

8.2.2 verify that you have entered the correct email addresses.

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 Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption you need to use the “Protect” button on the new email window. For more information about encrypting emails refer to the information on CLiF or speak to the CLF ICT Service team. 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:** If you have been provisioned a CLF email address for CLF related work, you must not use a private email address and you must only use the Office 365 email address provided by the CLF. In any event Personal Data must not be shared on personal email accounts. Please note that this rule applies to Governors or Councillors as well. Please speak to the CLF ICT Service Team 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 Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out below. Information must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (**DSL**) room. The cabinets are located around the CLF as documented in the information asset registers. Academies will maintain at least the following cabinets:

(a) Designated safeguarding lead’s file;

(b) Special education needs file;

(c) Student files;

(d) Archive student files;

(e) Staff files;

(f) Archive staff files;

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins. These bin are available in each academy and central offices. If you need help finding a secure bin contact your academy principal or central team manager. Personal Data should never be placed in the general waste or any disposal box from which the material can be easily recovered.

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 Data Protection Team.

9.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. In some cases 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 Personal Data. Please see paragraph 9.2 above for details of where Critical 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 your IT team 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. You must make sure that Personal Data taken off site is returned to the School.

10.3 If you are allowed to work from home then check with Data Protection Team what additional arrangements are in place. This might involve being given access to a remote portal to securely access CLF systems, please see section 11 below.

10.4 Not all staff are allowed to work from home. If in doubt, speak to the HR Director.

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

(a) particularly sensitive documents containing Critical Personal Data 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);

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

(c) 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;

(d) 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 **Using CLF laptops, phones, cameras and other devices:** If you need to book out a CLF device then liaise with the CLF ICT Service team.

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 school trips (see 10.5 above).

11 Using personal devices for CLF work

11.1 You may only use your personal device (such as your laptop or smartphone) for CLF work if you have been given permission by your academy principal or central team manager.

11.2 Even if you have been given permission to do so, then before using your own device for CLF work you may need to speak to your IT team to ensure you have access to a remote portal to securely access the CLF systems. If you need more information on securely access documents on personal devices speak with the CLF ICT Service team.

11.3 **Using your own PC or Laptop:** If you use your laptop or PC for School work then you must use the remote access software provided by the CLF known as the Remote Portal. Using the Remote Portal means that Personal Data is accessed through the CLF's own network which is far more secure and significantly reduces the risk of a security breach. If using the CLF systems in the cloud, such as Office 365, you must only view and edit documents within the browser. You must not download documents to your workstation. If you need more information on securely access documents on personal devices speak with the CLF ICT Service team

11.4 **Using your own smartphone or handheld:** Before you use your own smartphone or handheld for School work you must connect your device to your Office 365 email account. This will install the device management software provided by the CLF. This software will help keep Personal Data secure and separate from private files.

11.5 This software is called Outlook, which is available as an app to download. Alternatively using the built in email apps will also active the management software. The software has remote wipe functionality which can be invoked should the device be lost or stolen. The CLF reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for the CLF or on the CLF's behalf or which contains Personal Data. Although we do not intend to wipe other data that is private in nature (such as private photographs or private files or emails), it may not be possible to distinguish all such information from Personal Data in all circumstances. You should therefore regularly back up any private data contained on the device or keep private material separate via a partition that would not be remotely wiped in these circumstances.

11.6 You must not do anything which could prevent any software installed on your computer or device by the CLF from working properly. For example, you must not try and uninstall the software, or save CLF related documents to an area of your device not protected, without permission from the CLF ICT Service Team first.

11.7 **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.

11.8 **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.

11.9 **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 CLF ICT Service team. This is because anything you save to your computer, tablet or mobile phone will not be protected by the CLF'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 CLF 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.

11.10 **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. You must also make sure that your devices are not configured in a way that would allow someone else access to CLF related documents and information – if you are unsure about this then please speak to the CLF ICT Service team.

11.11 **When you stop using your device for CLF work:** If you stop using your device for CLF work, for example:

(a) if you decide that you do not wish to use your device for CLF work; or

(b) if the CLF withdraws permission for you to use your device; or

if you are about to leave the CLF then,

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

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

13 Appendix 1 CLF applications

Application	What it can be used for	Specific security arrangements	Any other notes / comments
CLF HR	Accessing and managing all processes in relation to staff.	Limited to specific staff. Only accessible from specific locations.	This system is hosted and managed in cloud via the provider.
Academy SIMS	Accessing and managing all processes in relation to students and staff within academies.	Different permissions to limit access are provided to staff as appropriate. Only accessible from specific locations or via the remote portal.	This system is hosted in academies or by the local authority. It is supported by the location authority support provider. All staff must ensure that passwords used on this system are long and complex.
Academy CPOMS	Reporting and managing incidents in relation to safeguarding.	Only limited access to staff to report incidents. Only designated staff are provided access to manage the details of the incidents and generate reports. Use of multi-factor authentication via a USB key is required designated staff.	This systems is hosted and managed in cloud via the provider. All staff must ensure that passwords used on this system are long and complex.
Office 365 (including Outlook email, OneDrive and 365 Groups)	All activity in relation to the creation, sharing and sending of emails and files such as documents, spreadsheets and presentations.	Staff are provided an account as required. Access to groups are limited to only those who are invited. Access to files is limited to only those with whom the file has been shared.	This system is hosted in cloud by Microsoft, but manage via the CLF ICT Service team. All staff must ensure that passwords used on this system are long and complex.