Cabot Learning Federation

Information Security Policy

Date Adopted: June 2020, Cabot Learning Federation
Implementation Date: June 2020
Updated: June 2024

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
09/06/2020	Whole document 1 2 6 8.1 12	Adjusted "critical data" definition to align with data protection policy. Include confidential information within scope following change from "critical data" Enhance examples of breaches Added reference to use of walkie-talkie Included section on email phishing, referencing safeguards in place to protect. Added section on training to ensure all staff complete.	
28/05/2024	Whole document	Merged with the Information Security for System Administrators and Password and Encryption policies.	

Contents

1 Policy Statement

2 Equalities Impact Assessment

An Equalities Impact Assessment has been carried out. The assessment concluded that there was no adverse impact identified for any groups of people with protected characteristics.

3 Policy Statement

3.1 Information security is about what you and the Cabot Learning Federation (**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.

3.2 This Policy has been created to ensure the CLF has the right controls in place to protect the Personal Data that it processes. However, the controls and requirements set out also protect confidential business information that is processed more widely. This includes data such as:

(a) CLF financial information;

(b) Strategic planning information;

(c) Detailed IT security information.

3.3 This policy should be read alongside the CLF's Data Protection Policy (DP Policy) which gives an overview of your and the CLF's obligations around data protection. The DP Policy can be found in the Policies section on any of the CLF websites and is also available on the CLF staff intranet, CLiF. In addition to the DP Policy, you should also read the following which are relevant to data protection:

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

(e) IT acceptable use policy in the Employment Manual.

3.4 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 DP Policy.

3.5 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 also works closely with the CLF Governance 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.

3.6 Questions and concerns about technical support or for assistance with using the CLF's IT

systems should be referred to the CLF IT Operations team via ITHelpdesk@clf.uk.

4 Roles and responsibilities

4.1 The board are responsible for the approval of this policy.

4.2 Academy Councils and Audit Committee are responsible for monitoring the implementation and application of this policy.

4.3 The IT Director is responsible for the implementation and application of this policy.

5 Be aware

5.1 Information security breaches can happen in a number of different ways. Examples of breaches which have previously occurred within CLF include:

(a) Sending a confidential email to the wrong recipient;

(b) Using carbon copy (CC) rather than blind carbon copy (BCC) to send emails to multiple recipients;

(c) Leaving confidential documents containing Personal Data on public transport;

(d) Losing confidential documents containing Personal Data on a school trip;

(e) Students accessing a staff members laptop after it was left unlocked when they left the room.

5.2 Poor information security leaves our systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

(a) identity fraud;
(b) targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
(c) witnesses put at risk of physical harm or intimidation;
(d) offenders at risk from vigilantes;
(e) exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence; and
(f) fake applications for tax credits.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

5.3 These should give you a good idea of the sorts of things which do go wrong, but please have a think about what problems might arise in your team or department and what you can do to minimise 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.

5.4 **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).

5.5 You must immediately tell the Data Protection Team or the CLF IT Operations 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.

5.6 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.

6 Thinking about privacy on a day to day basis

6.1 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.

6.2 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 or software which uses Personal Data, where the processing results in a risk to individual's privacy or where Personal Data is used on a large scale, such as CCTV.

6.3 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.

6.4 System that utilise artificial intelligence, such as generative AI or machine learning require large amounts of information on which to train or from which to provide a creative response. Any information shared with an AI system may breach information security controls and put the data at risk.

7 Special Category Personal Data

7.1 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 **Special Category Personal Data** in this policy and in the DP Policy. Special Category Personal Data would include:

(a) information concerning child protection matters;

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

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

(d) political opinions;

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

(f) trade union membership;

(g) physical or mental health or condition;

(h) genetic information;

(i) sexual life;; and

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

7.2 Staff need to be extra careful when handling Special Category Personal Data.

8 Minimising the amount of Personal Data that we hold

8.1 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 Records Retention Policy or speak to the Data Protection Team.

9 Using computers and IT

9.1 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:

9.2 **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 IT Operations team. The CLF's computers are configured to automatically lock if not used for 5 minutes. In some classroom settings this is extended to support learning. In these circumstances staff must also ensure workstations are locked when leaving them unattended.

9.3 **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 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.

9.4 Specific guidance on the information security requirements of the different programmes that the CLF uses can be found in section **Error! Reference source not found.** of this policy.

9.5 **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 IT Operations 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)".

9.6 **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store

or share CLF documents.

9.7 **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 Data** unless those devices have been approved by the CLF IT Operations 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 IT Operations team.

9.8 **Disposal of CLF IT equipment:** CLF IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the CLF IT Operations Team even if you think that it is broken and will no longer work.

9.9 **Walkie Talkies:** It should be assumed that discussions over walkie talkie equipment will be insecure. As a result, the full name of students must not be used in conversations, initials should be used instead. Staff must be careful to minimise the amount of information disclosed in conversations, adopting an attitude that assumes whatever they are saying can be overheard by others. Teachers surnames can be used in conversations.

10 Passwords

10.1 Passwords should be long, at least 10 characters, 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 IT Operations team.

10.2 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.

10.3 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.

10.4 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.

11 Artificial Intelligence

Artificial intelligence (AI) systems can enhance teaching, learning and administrative processes, but are known to have a number of limitations that present risks.

11.1 **Inaccurate or Misleading Information:** AI responses may not always be accurate or reliable. The models can generate incorrect information, misconceptions, or outdated content. Users must verify and cross-reference information from AI tools with reliable sources before sharing or considered as fact.

11.2 **Bias and Stereotyping**: AI tools learns from vast amounts of training data, which may contain biases present in society. Consequently, the models can inadvertently exhibit biased behaviour or reinforce stereotypes. Users should be aware of potential biases and actively address them

by providing diverse perspectives and inclusive content, encouraging critical thinking about bias and stereotypes.

11.3 **Technological Limitations**: AI tools have limitations in its understanding and context. It may struggle with ambiguous questions, complex reasoning, or nuanced interpretations (the ability to understand and appreciate the subtleties, complexities, or fine distinctions in a situation, statement). Users should be aware of these limitations and act accordingly as sometimes, tools like ChatGPT may not be the most effective tool.

11.4 **Lack of Accountability**: AI language models, like ChatGPT operate based on pre-trained algorithms and data. In case of errors, biases, or negative consequences arising from its responses, determining responsibility and accountability can be challenging. Users should be aware of this lack of accountability and take responsibility for the interactions and content facilitated through AI tools like ChatGPT.

11.5 **Data privacy and security:** Cybersecurity measures are implemented to prevent data breaches and unauthorised access to sensitive information, including AI-generated content. A number of security controls are in place, including mandatory data protection training, that limits how data is stored and shared. Users must ensure that **NO** personal or business confidential data is shared during interactions with any AI tool, unless there is a clear business case demonstrated through a Privacy Impact Assessment.

12 Emails (and faxes)

12.1 **Phishing**: This is a type of cyber attack where a malicious email is sent that pretends to be someone else. The email address of the sender may on the surface look like someone within CLF or someone else you communicate with. These emails attempt to lure the recipient into disclosing information such as usernames and password with a call-to-action. This might be a demand to update your account information or change your password.

12.1.1 If in doubt, right-click on the email address of sender to find out more information or contact the Cyber Security Team on spam@clf.uk.

12.1.2 All emails that originate from outside the CLF will be marked as such at the top of the email message that you receive.

12.1.3 If you receive a message that maybe a phishing attack forward the message to spam@clf.uk

12.2 When sending emails or faxes you must take care to make sure that the recipients are correct.

12.3 **Emails to multiple recipients:** When sending email to multiple recipients liaise with the CLF IT Operations 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:

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

12.3.2 verify that you have entered the correct email addresses.

12.4 If the email or fax contains Special Category 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 Special Category Personal Data then you should make sure that the intended recipient is standing by the fax machine to receive the fax.

12.5 **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 IT Operationsteam. 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.

12.6 **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 IT OperationsTeam if you require an email account to be set up for you. Staff are not permitted to set up "forwarding" from their CLF address to any private email addresses. Attempts to set up any form of forwarding are monitored and will be limited.

13 Paper files

13.1 **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.

13.2 If the papers contain Special Category 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;

13.3 **Disposal:** Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins or shredding them using CLF shredders. Bins 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.

13.4 **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 or dispose of it in a confidential waste bin.

13.5 **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 Special Category Personal Data. Please see paragraph 13.2 above for details of where Special Category Personal Data should be kept.

13.6 **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.

14 Working off site (e.g. School trips and homeworking)

14.1 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.

14.2 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.

14.3 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 15 below.

14.4 Not all staff are allowed to work from home. If in doubt, speak to the relative Principal or Director.

14.5 **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 information about pupil medical conditions (for example allergies and medication) with them. 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.

14.6 **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 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.

14.7 **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 Special Category 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 14.5 above).

14.8 **Using CLF laptops, phones, cameras and other devices:** If you need to book out a CLF device then liaise with the CLF IT Operationsteam.

14.9 Special Category 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 14.5 above).

15 Using personal devices for CLF work

15.1 When you enrol onto your CLF Microsoft 365 account for the first time you will be required to install the Microsoft authenticator app onto your personal phone. This will ensure your personal details, including payslip, are secured via multi-factor authentication. The Authenticator app is used by lots of apps to help secure your data and it is likely that you already have it installed to protect other apps that store your information.

15.2 **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 own devices**. If you need more information on securely access documents on personal devices speak with the CLF IT Operations team.

15.3 **Using your own smartphone or tablet:** Before you use your own smartphone or tablet for School work you must connect your device to your Microsoft 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.

15.4 The Microsoft 365 apps are available to download from app stores. When you log in it will active the device management features within the app. 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.

15.5 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 IT Operations Team first.

15.6 **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. The CLF provide anti-virus software including a firewall, free of charge, to all CLF students and staff. Further details of this can be found on CLiF.

15.7 **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 10 above for guidance on choosing a strong password.

15.8 **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 IT Operations 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.

15.9 **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 IT Operations team.

15.10 **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

(c) 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 IT OperationsTeam for wiping and software removal. You must provide all necessary co-operation and assistance to the CLF IT Operations Team in relation to this process.

16 Training

16.1 All staff must complete the mandatory Data Protection and Information Security Essentials training as part of their initial induction and annually thereafter. The material can be access from the CLF training platform Nimble. The CLF reserve the right to request staff revisit this training in addition to the annual refresher training.

17 Breach of this policy

17.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

17.2 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 and reporting to the Information Commissioner for consideration of criminal action.

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

17.4 We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

18 Information System Administrators

The following sections are for owners and managers of information systems. This includes principals and directors, and any members of staff than oversee the administration of a Critical Information System. Such individuals will be identified and made part of the Information Security for System Administrators network.

18.1 Management direction for information security

The remainer of this policy describes controls that must be overseen by individuals that own or manage access into critical information systems.

This policy is based on standards and definitions from the ISO27001 and the GOV.UK service manual for Information Security. It is divided into a number of sections as defined by ISO27001 and supported by security controls in use throughout the CLF and supplier organisations.

There are a number of supporting policy documents that are referenced:

- Data protection policy
- Data retention policy

19 Organisation of information security

19.1 Information classification

The Information Security Policy is concerned with both Personal Data (as defined in the Data Protection Policy) and confidential business information (Confidential Information).

Confidential Information is of significant value to the CLF; the loss of which could result in an inability to carry out core purpose, negative publicity, additional costs, regulatory actions or fines.

All IT equipment owned or operated by CLF are Hardware Assets of the CLF.

All software owned or licensed by CLF are Software Assets of the CLF.

The contents of all digital forms of information, including databases, mailboxes, word processed documents, spreadsheets, web pages, data files or configuration files, created by staff, students, Academy Councillors, Board members or third parties in the course of their duties are Information Assets of the CLF.

All such assets are collectively referred to as Assets and must be accounted for and have a nominated owner.

This policy is specifically concerned with the controls in place to safeguard Critical Information Systems. Such systems can be identified as:

- containing Personal Data or Confidential Information,
- are made available through user access controls to many members of staff, and
- are critical to the functioning of an academy or CLF.

19.2 Internal organisation

This policy is designed to ensure adequate controls and management processes are in place on all Critical Information Systems across the CLF, regardless of the academy or team that own or operate the system.

This policy must be read and followed by all staff that administer access into or maintain a Critical Information System that contains Personal Data or Confidential business information. Such administration would include:

- super-user access into a system (i.e. they can access all information within that system)
- management of user accounts that permit others access to information within that system.

The three key roles that support the implementation of this policy are:

The Information System Owner (ISO) - the person that is accountable for maintaining the security of the system. Examples include an academy Principal or department Director.

The Information System Manager (ISM) - the most senior super-user that performs the daily management of the system. Examples include a Network Manager or Bromcom Manager.

The Information System Administrator (ISA) – any other users, that has super-user access or administers other user accounts within that system. Examples include an IT technician or Admin Assistant.

Examples of such systems within the CLF include:

- HR system (Access People)
- Network directory (Active Directory/Office 365)
- School management information system (SIMS)
- Finance system (Access Financials)

Information can be stored on computers, transmitted across networks, held on paper, held on digital removable media and transmitted in conversations. All forms of information must be protected.

The growth of distributed networks and cloud systems presents opportunities for unauthorised access to computer systems. As personal mobile devices become more prolific, access to systems can take place on many devices outside the management scope of the CLF ICT Team. As such there is a greater need for departments and employees to take appropriate responsibility for safeguarding the security of our systems.

Information security refers to the theory and practice of defending data or information systems against:

- Unauthorised or unintended access
- Destruction
- Disruption
- Tampering

There are 3 main concepts that support the management of information security. These consist of:

- **Confidentiality** - the assurance that information is not disclosed to individuals or systems that are not authorised to receive it
- **Integrity** - the assurance that information cannot be modified by those who are not authorised to modify it, or that any such modifications will not pass undetected
- **Availability** - the assurance that information is available when it is needed, and that mishap or malice cannot affect the ability of systems to provide information when requested

The CLF will use a number of controls to support the management of information security which include:

- Physical, such as walls and locked doors
- Procedural, such as training and processes
- Regulatory, such as policies and rules of conduct
- Technical, such as cryptographic software or use of secure protocols

The Information Security for System Administrators Policy ensures business continuity and minimises business damage by preventing and diminishing the impact of security incidents. The policy enables information to be accessible, but ensures the protection of that information and related ICT assets.

19.2.1 ICT Operating Standards

The CLF ICT Team maintain a detailed knowledge base on the implementation of certain controls. Standards marked as mandatory must be followed. These are listed within the Appendix.

19.2.2 Information security working group

An Information Security Working Group, formed from ISMs across the CLF, will meet to facilitate training of ISMs, maintain and support the controls in place across systems and continually enhance all areas of information security across the CLF.

20 Human resources security

20.1 Prior to employment

Information security responsibilities must be considered during recruitment processes for staff that will be required to administer or maintain a Critical Information System. This must be facilitated through job descriptions and pre-employment screening.

An introduction to the requirements of this policy must be included in the induction process.

20.2 During employment

Members of the Information Security Working Group will collaborate to continually test and evolve practice related to this policy.

ISM/ISAs must not assume authorisation to administer a system or to access Personal Data or Confidential Information, where administrative privilege enables such access. When in any doubt the ISO must be informed and support requested if required. Use of administrative privilege to gain access

to Personal Data or Confidential Information beyond that which is reasonably required may be considered a breach of the Employee Code of Conduct.

20.3 Termination and change of employment

On termination of contract, ISM/ISA accounts must be disabled immediately.

For all staff, users accounts must be disabled but remain complete for a minimum of 30 days. The user account will then be subject to the leaver process. Disabled and de-activated users may only be reactivated for administrative purposes, for temporarily accessing and moving resources or if the staff member has returned.

21 Asset management

21.1 Responsibility for assets

The ISM is responsible for and will maintain information about all associated Critical Information Systems within the information systems inventory (the Inventory). The Inventory will clearly identify owner and purpose. The minimum data items captured per Asset is listed in the Appendix.

It is the responsibility of the ISM of an asset to:

- ensure any changes to configuration, usage or location are approved and reflected in the Inventory
- ensure that access to the Assets for which they are responsible is controlled and managed in accordance with this policy

22 Access control

22.1 Business requirements of access control

CLF will provide all staff, students, Academy Councillors, Board members and third parties with access to information they need to carry out their responsibilities.

Access to information must be appropriately controlled according to the content, information classification and the methods which are deemed acceptable for access.

Access control standards will include explicit logon to devices, Microsoft Windows shares and file permissions; user access privileges; server and workstation access rights; firewall permissions; Microsoft Active Directory group membership; database access rights; Wi-Fi authentication; encryption and other mechanisms.

22.2 User access management

22.2.1 Access policy

Access to Information Assets will be controlled by the ISM who must ensure there is an appropriate business need for such access. Controls for access will include:

- registering authorised users and defining access permissions
- ensuring users are aware of their responsibilities for information security and data protection
- ensuring suitable network access control is part of the network operating systems
- restricting access to Personal Data and Confidential Information
- monitoring usage of specific resources
- reviewing users and user access permissions regularly

22.2.2 Managing user access

Access to Critical Information Systems will be provided through authentication and authorisation mechanisms such as a unique user ID and complex password.

Staff user accounts must be requested and processed through the related ISM. User accounts for leavers or changes must be promptly disabled or updated to account for changes to access permissions.

22.2.3 Managing passwords and Multi-factor Authentication (MFA)

All passwords must be issued, distributed and managed in a secure manner, ensuring that passwords are not disclosed to others in transit. Wherever possible initial passwords should be updated by the user on first login.

When setting end-user passwords and where possible, password complexity must be implemented and focus around length, using a minimum of 10 characters.

Wherever possible all user identifies should be integrated into the CLF M365 identity system, thus minimising the number of credentials used and enabling the common MFA system.

If integration into the CLF M365 identity cannot be established, MFA must be enabled where personal or business confidential information will be accessible.

System administrator passwords must be:

- at least 10 characters in length;
- contain a mix of upper and lower case letters;
- Use one or more numbers or symbols.

Password managers are permitted, but must be secured via MFA.

22.3 User responsibilities

All staff receive annual training in respect of Data Protection and Information Security. The Information Security for Staff Policy details the controls in place for securing passwords, locking working stations, and the risks around threats such as phishing.

ISMs must receive additional training to understand the risks in relation to security and to embed the controls within this policy. This training will form part of the Information Security Working Group.

ISMs must ensure staff granted access to information systems understand their duties and responsibilities in keeping the information secure.

Any breaches of information security must be reported to the CLF ICT Team, if the breach concerns Personal Data the CLF Data Protection Team must be informed.

Any staff that identifies a present or potential threat to information security should inform the CLF ICT Team or the CLF Data Protection Team immediately.

22.4 System and application access control

22.4.1 Management duties

The allocation of super-user permissions such as local administrators, domain administrators, and system managers must be restricted and only permitted where necessary.

Super-user accounts must be assigned to individuals only and not shared. Use of generic administrator logins on information systems containing Personal Data or Confidential Information must not be used for regular, routine operations and wherever possible must be disabled when not in use.

22.4.2 Third party service management

Third parties are provided accounts that permit access to systems and information in order to provide support and maintenance of the systems.

At the end of the contract period accounts will be disabled and deleted as defined for staff accounts.

Unless operationally necessary, third party accounts will be disabled when not in use.

22.4.3 Non-named accounts

Generic or group user accounts must only be granted if sufficient controls are in place to secure access to the accounts. These controls may include an encrypted password database.

22.4.4 Service accounts

Service user accounts created for the purpose of scheduling automated processes or to give applications the security privilege to function, must be configured with the minimal set of access required.

23 Cryptography

23.1 Cryptographic controls

23.2 Only modern industry standard algorithms should be used for encrypting and signing of information. Applications and services must be regularly patched with security updates and thus insecure or depreciated protocols will eliminated.

23.3 Email services must use opportunistic TLS when connecting to third parties, except in cases where there has been an identified need to ensure all traffic is encrypted between email servers. In these cases, TLS encryption must be enforced between specific endpoints.

23.4 End-user devices, such as laptops and desktops, that have been identified as requiring hard disk encryption must be configured with a minimum 256-bit key.

23.5 Mobile phones and tablets must be encrypted with the mandatory built-in encryption software and kept up to date.

23.6 VPN and network encryption services must be fully up to date and encrypted with a minimum 128-bit key.

23.7 Vulnerable and depreciated protocols such as SSL, TLS1.1 or below and SMB 1.0 must not be used and disabled if necessary.

24 Physical and environmental security

24.1 Secure areas

24.1.1 Physical security

ICT equipment supporting critical business activities must be housed in secure areas protected from unauthorised access, damage and interference. Systems must be protected by a defined security perimeter, with appropriate entry controls, security barriers and any specific environmental conditions recommended by the manufacturer or supplier.

Server rooms must remain locked when not in use. Where servers are not placed in dedicated rooms they must be secured within locked cabinets.

Where this provision is not available an action plan will be drawn up and implemented to reduce the risk.

24.1.2 Controlling data distribution

Critical information must remain in known, compliant locations at all times. Where information is moved between locations for operational or maintenance purposes any transient locations must provide the minimum level of protection set out in this policy.

Where data is digitally transferred between locations the data must be encrypted in transit.

24.2 Equipment

1.1 Taking equipment off the premises

Any devices that are to be used outside of CLF premises and contain critical information must be protected from unauthorised access. In the case of mobile laptop devices these must be encrypted to a level as defined this policy.

ISMs must ensure that data processed on devices outside of CLF premises are secured.

In the event that a mobile device containing Personal Data or Confidential Information is lost or stolen, the ISM for that information and the CLF IT Team must be informed immediately.

Special care must be taken to protect mobile devices (laptops, mobile phones, USB keys, PDAs etc.), due to the relative ease with which these may be stolen. ISM must refer users of such devices to the Information Security for Staff policy and reminded to:

- never leave them unattended in a public place
- not loan mobile devices to friends or family members
- never leave equipment visible in a parked car (i.e. always leave equipment out of sight in the boot)
- take reasonable steps to secure equipment away at night if left in the office or home

24.3 Removable media

Digital removable media such as USB sticks must not be used as a permanent means for storing information, due to their reduced reliability and vulnerability to loss. In cases where digital removable media are required for temporary storage, Personal and Confidential information must only be stored on devices that are encrypted to a level as defined in this policy.

24.4 Decommissioning of equipment

Devices with storage including servers, storage-area-networks, workstations and laptops must be securely wiped prior to disposal. Reputable disposal companies with appropriate certification may be employed to both dispose and securely wipe disks, providing a certificate of this process.

25 Operations security

25.1 Operational procedures and responsibilities

Operating procedures and detailed instructions must be in place for all information systems, to ensure their correct and secure operation. Documented procedures are also required for any systems development, maintenance and testing, especially where it involves cross-functional activities with other groups.

Where the nature of the roles within a team provide sufficient knowledge of the build and operation of a system a minimum level of documentation is required for core elements of administration and maintenance.

System documentation should include the following:

- Initial setup or configuration information

- Inter dependencies with other parts of the ICT infrastructure
- Support contacts
- Back up and system recovery procedures
- Relevant operating procedures
- Super-user username information and credentials stored in secure locations or in escrow

25.2 Protection from malware

25.2.1 Installing virus scanning software

All networks systems, servers and managed devices should have anti-virus software installed to reduce the risk of malware infection.

Anti-virus systems servers should be configured to received definition updates on at least an hourly basis.

These systems should be regularly monitored.

25.2.2 Combating cyber crime

ISMs must be aware of the threat of cyber-attacks, particularly as they may be a target for such attacks in order to disrupt or gain access to information. Such awareness must be included in the ISM training programme.

Such attacks include:

- Phishing – where a user receives an email or is manipulated into entering username and password into a fake website. This would result in the disclosure of the username and password.
- Social engineering – phishing in person – where someone pretends to be from a company who supports a system and asks for access to a server room or to access a system. Never provide access to systems unless the identity of the requester can be authenticated and is genuine.
- Denial of service attacks – where a system is targeted by multiple malicious entities on the Internet so as to overload a system and make it inaccessible. Reasonable measure must be in place to detect and deflect such attacks.
- Ransomware (and malicious software) – where a user accidentally runs an application on a network that is designed to disrupt or extract data from a system. Ransomware, a common example of such a threat, encrypts all data on devices it can access and demands payment before providing the decryption key. Only approved software is permitted on CLF devices and additional safeguards must be in place to protect against such threats.

25.2.3 System utilities

To reduce the risk of malicious software, only well known, standard system utilities should be used for maintaining information systems.

Scripts downloaded to provide administrative tasks must be reviewed in detail to be assured it functions as expected.

25.3 Backup

The ISMs must ensure there is an appropriate disaster recovery process in place to protect all information systems.

These systems must be documented, tested and reviewed regularly.

CLF hosted systems must be backed up and operate the 3-2-1 backup rule:

- 3 copies of the backup data
- 2 copies on different storage media
- 1 copy located offsite or within a separate building to the main store.

For externally hosted systems it must be possible to demonstrate that reasonable safeguards are in place to maintain access to the system without disruption.

Backup safeguards must be noted in the Inventory.

25.4 Logging and monitoring

Critical Information Systems must provide information on usage. This may be in the form of logs of successful and failed login attempts. These should be reviewed regularly.

All end-user workstations should have appropriate monitoring and management tools in place to support the safeguarding of staff and students.

25.5 Control of operational software

25.5.1 Controlling access to operating system software

Where required on user assigned devices, individual users may be delegated local administrative permissions.

25.5.2 Restricting execution of unauthorised applications

All end-user Windows workstations should have controls in place to limit the applications that can be executed by user. Standard Windows software restriction settings should be in place to support this. Workstation Monitoring and Management

All end-user workstations should have appropriate monitoring and management tools in place support the safeguarding of staff and students.

These tools must log workstation usage, including logon/logoff events and applications usage.

25.5.3 Securing unattended devices

All devices must be secured when not attended. Administrative controls must be in place to support such capability. Such controls include screensaver locks and PIN policies on mobile devices.

All users must lock workstations when leaving unattended.

25.5.4 Mobile device protection

Any mobile devices connecting to email systems must be protected via passcode and auto-lock timeout. The system must have a capability to auto erase the device in the event of loss.

25.6 Technical vulnerability management

Information systems, core applications and the operating systems of all servers and user devices must be kept within serviceable versions of the vendor.

Information systems, operating systems and core applications must be continuously upgraded with critical security updates from the vendor.

26 Communications security

26.1 Network security management

26.1.1 Internet and network connectivity

Where an Internet connection is provisioned within a CLF site reasonable safeguards must be in place to protect against cyber-attacks and to provide an appropriate level of filtering.

All Internet firewalls must log Internet access, where possible via an associated IP address or username.

26.2 Managing network access controls

Reasonable measures must be taken by all ISMs to ensure that Critical Information Systems are secured at the network layer, through the use of firewall systems and appropriate network segregation.

ISM that are not part of the CLF IT Team should liaise with this team for assurance that such measures are in place on systems they manage.

Systems hosted by a third-party must demonstrate reasonable controls are in place to encrypt and protect data within the systems. This may include conformance to standards such as ISO 27001.

26.3 Sharing information

When any user sends information to any other user either internally or externally, steps must be taken to ensure that the information is secured during transit and that personal and confidential information will not subsequently reside in a location that would put the information at risk.

The sharing of Personal Data and Confidential Information is not recommended by email, unless the recipient is within the organisation or the information is encrypted to a level as defined in this policy

Where the recipient is outside of CLF the recipient address must be validated as correct.

27 System acquisition, development and maintenance

27.1 Security requirements of information systems

27.1.1 Purchasing and installing software

The procurement of new Critical Information Systems must be subject to a review to determine all information assets are appropriately secured. Such a review must include the CLF IT Team. Any new systems which will process Personal Data must complete a Data Protection Impact Assessment in conjunction with a member of the Data Protection Team.

All software and information systems purchased must be logged in the Inventory, ensuring that relevant ownership, purpose and expiry information is captured.

It is the responsibility of the identified owner of the software to ensure that any license is renewed with the support of the CLF IT service if required.

27.1.2 Using licensed software

All licensed software should be inventoried and reviewed regularly.

Where a software license has expired the ISOs must ensure any related software is uninstalled in line with the license agreement, or renew the agreement.

27.1.3 Managing electronic keys

All keys used for securing information or licensing software must be securely stored and logged within the Inventory, to identify the location.

This includes security certificates used on websites and license keys for software.

The Inventory information should indicate any expiry dates, to facilitate the proactive maintenance and renewal of services.

27.2 Security in development and support processes

Updates, configuration changes and operational maintenance should be undertaken in a controlled manner. The ISMs must ensure appropriate testing, backups and roll-back capabilities are implemented.

27.3 Test data

Test data used when installing, updating or testing a system must be carefully selected so as not to inadvertently expose Personal Data or Confidential Information.

28 Information security incident management

28.1 Management of information security incidents and improvements

If a breach of information security has been identified the CLF IT Team must be informed, who will then investigate and take appropriate action.

If necessary the CLF Data Protection Team and the related ISM will support the investigation and any follow up action.

29 Information security aspects of business continuity management

29.1 Information security continuity

Business continuity planning is a necessary process for all CLF teams. The confidentiality, integrity and availability of all information systems is critical to maintain business continuity.

All ISMs must support the business continuity planning through the regular review of the Inventory. Accuracy in the measures stated in respect of recovery processes and failover systems is crucial for ensuring that plans operate as expected, minimising downtime and disruption during any event.

The Inventory must state an estimated recovery time in the event that a system restore or failover is required. Where a system is not hosted by CLF, references to contractual SLAs must be noted.

29.2 Redundancies

Critical Information Systems hosted by CLF should have reasonable redundancies in place to protect against common incidents. The inclusions of such redundancies should be evaluated in terms of the risk an incident against the cost of any redundancy and alternative contingencies.

Typical redundancies that should be considered will include:

- Disk redundancies to protect against a failure of an individual disk
- Server failover to protect against a server malfunction
- Core networking redundancies, to provide multiple routes for network connections from server to the rest of the network

30 Appendix

30.1 CLF IT Operating Standards

The CLF IT Operating Standards contain detailed information in relation to Information security controls identified within this policy. These standards must be regularly reviewed and are available within CLF IT Operations Area.

a) Data backup and recovery

b) Device encryption

c) Administrative user accounts

d) Forced password changes

e) Internet filtering

f) Microsoft licensing distribution

g) New starter process

h) Procurement of devices, servers and infrastructure (Inc. preferred model list)

i) Screen saver timeout

j) Server room layouts and security

k) Software restrictions

l) System monitoring

30.2 Inventory template

The Information Security Asset Inventory (Inventory) must capture at least the following data items for each asset:

Item	Notes	Examples
System name		SIMS, Active Directory
Purpose	If not obvious from name.	Capture and manage after school activity information.
ISM	The name of the person responsible for maintaining access into the system. If multiple people can provision access to the system list additional names. The first name is considered the ISM.	Name of SIMS manager, Name of Network Manager
Date of license renewal		
Cost of last renewal		
Date of next renewal		

License key location	If relevant, where is the latest key stored?	IT KeePass DB
Location of host	Which building and room is the system hosted in? This may be cloud.	
Physical security	Describe how the asset is physically secured.	Server cabinet, Server room with lock and key, Key in key safe
Disaster recovery method	What is used to backup and recover the system? If cloud based, detail the controls or standards in place as described within the contract.	Veam, Microsoft DPM, Cloud – secured to ISO27001
Disaster recovery time	What is the estimated restore time for this system. This time should assume a recovery from the remote location. Reference latest DR tests. If cloud based, detail the SLA for system uptime.	6 hours.
Disaster recovery location	Which building and room is the backup stored in?	
Disaster recovery physical security	Describe how the asset is physically secured.	Server cabinet, Server room with lock and key, Key in key safe
Disaster recovery 3-2-1	Is the 3-2-1 method in effect? (3 copies, 2 media, 1 in remote location)	Yes/No