Snowdon Village

POSITIVITY | EQUITY | RESILIENCE | LOVE

Cabot Learning Federation

Data Protection Policy for Staff

Date Adopted: June 2022, Cabot Learning Federation

Implementation Date: June 2022

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 document	
06/03/2018	Whole document	Updated following review from DP working groups	
01/05/2018	1.2 3.8 and 3.9 4.11 4.2.1 a) 6.1 9.1	Removed section explaining the CLF and relationship to schools. Change of definition of “special data” to the broader definition of “critical data". Added point e) and f) Updated to refer to guidance in the UK GDPR FAQ document. Added to provide clarity around the sharing of data. Additional wording.	Review from VWV
25/06/2020	Whole document	Annual Review Creation of standalone Policy Reference to new Special Category Data Policy Addition of Policy Equality Impact Screening	
24/06/2021	Whole document	Annual Review Clarification on the role of the DPO Addition of CLF approach to handling Processors; Standard Contract Clauses being required to safeguard overseas transfers; and Data Privacy Impact Assessments for high risk processing	
23/06/2022	Whole document	Annual Review Minor changes made following completion of ICO Accountability Assessment, including DPO reporting to member of Exec Team, link to SAR Procedure and DPO contact details.	

Contents

1 Introduction

1.1 This Policy is about our obligations under data protection legislation, in particular the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DP Act 2018). Data protection law regulates the way Cabot Learning Federation (the **CLF**) processes information about living, identifiable individuals (Personal Data). It also gives individuals various rights for example the right to access their Personal Data and the right to request the erasure of Personal Data they no longer want us to process and which we no longer need to retain.

1.2 We will collect, store and process Personal Data about our staff, pupils/students, parents/carers, suppliers and other individuals who come into contact with the CLF. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the CLF and will ensure that it continues to operate successfully.

1.3 The CLF has appointed a Data Protection Officer (DPO) who is responsible for monitoring our compliance with Data Protection laws, informing and advising on our data protection obligations, providing advice regarding Data Protection Impact Assessments and acting as the primary point of contact for Data Subjects and the Information Commissioner's Office. The DPO can be contacted using the following email address - dataprotection@clf.uk.

1.4 The DPO will report to a member of the CLF Executive Team.

1.5 Each academy and central function has a designated Data Protection Lead. The DPO works closely with the CLF Corporate Services team in relation to some data protection functions. Together the DPO, Corporate Services team and Data Protection Leads are referred to as the **Data Protection Team**. All queries concerning data protection matters must be raised with an appropriate member of the Data Protection Team, this will often be the relevant Data Protection Lead in the first instance.

2 Application

2.1 This Policy is aimed at all staff working in the CLF (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes staff, governors, contractors, agency staff, work experience or placement students and volunteers.

2.2 In order for you to do your job, you will likely need to access, process, disclose, procure or delete Personal Data. You must only use Personal Data for valid business or legal reasons.

2.3 You must comply with this Policy when processing Personal Data. Any breach of this Policy may result in disciplinary action.

2.4 This Policy does not form part of your contract of employment and may be amended by the CLF at any time.

3 What information falls within the scope of this Policy?

3.1 Data protection concerns information about living, identifiable individuals. Companies and legal entities are not protected by the legislation, but must comply with it.

3.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is readily available, regardless of the media it is recorded or held on (i.e. paper and electronic formats). Information as simple as someone's name and address is their Personal Data.

3.3 The following are referred to as Special Category Data in this Policy and in the Information Security Policy. You must be particularly careful when dealing with this type of information because it is considered to be particularly sensitive:

(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) information about an individual's racial or ethnic origin;
(e) political opinions;
(f) religious beliefs or other beliefs of a similar nature;
(g) trade union membership;
(h) physical or mental health or condition;
(i) sexual life;
(j) genetic information;
(k) information relating to actual or alleged criminal activity; and
(l) biometric information (e.g. a pupil's fingerprints to securely manage dinner money payments).

3.4 Examples of places where Personal Data or Special Category Data might be found are:

(a) in a computer database or application systems (e.g. SIMS, CPOMS, Show My Homework and Access HR);
(b) in a manual file, such as a pupil or staff member record;
(c) a register or contract of employment;
(d) pupils' exercise books, coursework and mark books;
(e) health records;
(f) email correspondence;
(g) a record about disciplinary action taken against a member of staff;
(h) photographs or CCTV (*);
(i) a tape recording of a job interview;
(j) contact details and other personal information held about pupils, parents and staff and their families and a member of the public who is enquiring about placing their child at the CLF; and
(k) information on a pupil's performance.

(*) NOTE: A separate Policy exists for the management of CCTV images, which is located in the Employment Manual, along with a supporting procedure to be used by staff operating and managing access to such equipment.

3.5 These are just examples - there may be many other things that you use and create that would be considered Personal Data or Special Category Data.

3.6 Some of the conditions for processing Special Category Data and criminal offence data, set out in Schedule 1 of the DP Act 2018, require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 of the UK GDPR and policies regarding the retention and erasure of such Personal Data.

A copy of the Special Category Data Policy must be made available to the Information Commissioner's Office (the UK data protection regulator) upon request and is available from the DPO.

4 Your Obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

4.1.1 Individuals must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have, how long we keep Personal Data for and their right to complain to the Information Commissioner's Office.

This information is often provided in a document known as a privacy notice or privacy statement. Copies of the CLF privacy notices can be obtained from the Data Protection Team or accessed from the CLF's public websites.

If you are using Personal Data in a way which you think an individual might conclude is unfair, please speak to the Data Protection Team.

4.1.2 You must only process Personal Data for the following purposes:

(i) ensuring that the CLF provides a safe and secure environment;
(ii) providing pastoral care;
(iii) providing education and learning for our pupils;
(iv) providing additional activities for pupils and parents (for example activity clubs);
(v) protecting and promoting the CLF's interests and objectives (e.g. fundraising);
(vi) safeguarding and promoting the welfare of our pupils;
(vii) managing the hire and use of CLF premises; and
(viii) to fulfil the CLF's contractual and other legal obligations.

4.1.3 If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Data Protection Team. This is to make sure that the CLF has a lawful basis for using Personal Data.

4.1.4 We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you must speak to the Data Protection Team if you think that you may need to use consent as the basis for processing.

4.2 Personal Data must be processed for limited purposes and in an appropriate way

Personal Data can only be used for a new purpose if it is either compatible with the original purpose for processing, we get consent from the Data Subject, or we have a clear obligation or function set out in law.

For example, if staff are told that they will be photographed to help create security passes, we must not use those photographs for another purpose (e.g. for promotional purposes in the CLF's prospectus) unless we obtain their consent or other laws allow us to use the images in this way.

4.3 Personal Data held must be adequate, relevant and limited to that which is necessary in relation to the purposes for which it is being processed

4.3.1 The Personal Data we collect and hold must be no more than is absolutely necessary to achieve our aims. For example, you must only collect information about a pupil's medical history if that Personal Data has some relevance, such as allowing the CLF to care for the pupil and meet their medical needs.

4.3.2 Decisions impacting individuals must not be based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil.

4.3.3 Changes to the way in which Personal Data are processed (i.e. the introduction of new software programs or Processors) must be subject to a suitable risk assessment which identifies the data protection risks associated with the change and the required controls which need to be implement to ensure compliance with data protection laws.

4.4 Personal Data must be accurate and kept up to date

You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you must update the CLF's information management system as soon as possible and not just as part of any annual refresh exercise.

4.5 Personal Data must not be kept for longer than is necessary

The CLF has a Records Retention Policy which states how long different types of data must be kept for and when it must be destroyed. This applies to both paper and electronic records. You must be particularly careful when deleting data, to ensure that it is securely destroyed.

Please speak to the Data Protection Team for guidance on the retention periods and secure deletion.

4.6 Personal Data must be processed securely

4.6.1 You must comply with the following CLF policies and guidance relating to the handling of Personal Data:

(a) Information Security Policy;

(b) IT Acceptable Use Policy for staff; and

(c) Records Retention Policy.

4.6.2 All staff must complete the mandatory Data Protection Essentials training as part of their initial induction and annually thereafter.

4.6.3 You must report any Personal Data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data immediately, using the Personal Data Breach Reporting Form. The Data Protection Team will ensure that it is captured on the CLF Breach Log and is escalated appropriately. Data breaches will include access to Personal Data by an unauthorised third party, sending Personal Data to an incorrect recipient, computing devices containing Personal Data being lost or stolen, alteration of Personal Data without permission and prolonged loss of availability of Personal Data.

4.6.4 Where Processors are engaged to process Personal Data on behalf of the CLF (e.g. software providers who host applications or confidential waste supplies), they must provide sufficient guarantees around compliance with the UK GDPR and that the rights of Data Subjects will be protected.

4.6.5 Where a Processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.

4.6.6 Where the CLF uses a Processor, a written contract with compulsory terms, as set out in Article 28 of the UK GDPR, must be in place (plus any additional requirements that we determine).

4.6.7 Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a Data Protection Impact Assessment (DPIA) must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect Personal Data.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance.

4.7 Personal Data must not be transferred outside the European Economic Area (EEA) without adequate protection

4.7.1 If you need to transfer Personal Data outside the EEA please contact the Data Protection Team. For example, if you are arranging a school trip to a country outside the EEA or you are planning to install software which will be hosted in the United States.

4.7.2 Standard Contract Clauses must be used where it is necessary to transfer Personal Data to 'third countries'. The reason for this is to ensure Data Subjects are granted a level of protection equivalent to that guaranteed by the UK GDPR.

5 Sharing Personal Data Outside the CLF – Do's and Don'ts

Please review the following do's and don'ts:

5.1 **DO** familiarise yourself with the guidance document entitled Handling Disclosures of Personal Data, which is available from CLiF or from your Data Protection Lead.

5.2 **DO** share Personal Data on a need to know basis - think about why it is necessary to share Personal Data outside of the CLF - if in doubt - always ask a relevant person from the Data Protection Team for guidance.

5.3 **DO** encrypt emails which contain Special Category Data described in paragraph 3.3 above. For example, encryption must be used when sending details of a safeguarding incident to social services.

5.4 **DO** make sure that you have permission from your manager or the Data Protection Team to share Personal Data on the CLF website.

5.5 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from individuals or organisations. You must seek advice from the Data Protection Team where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

5.6 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for Personal Data or financial information or click on any links in an

email from someone that you don't recognise. Report all concerns about phishing to the Central IT team.

5.7 **DO NOT** disclose Personal Data to the Police without permission from the Data Protection Team (unless it is a life and death emergency).

5.8 **DO NOT** disclose Personal Data to contractors without permission from the Data Protection Team. This includes, for example, sharing Personal Data with an external marketing team to carry out a staff recruitment event.

6 Sharing Personal Data Within the CLF

6.1 Personal Data must only be shared within the CLF on a "need to know" basis.

6.2 Examples of sharing which are **likely** to comply with the data protection legislation:

(a) a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);

(b) informing an exam invigilator that a particular pupil suffers from panic attacks;

(c) and disclosing details of a teaching assistant's allergy to bee stings to staff members so that you/they will know how to respond (but more private health matters must be kept confidential).

6.3 Examples of sharing which are **unlikely** to comply with the data protection legislation:

(a) informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

(b) disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

6.4 You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the Designated Safeguarding Lead as a matter of urgency.

7 Individuals' Rights in Respect to Their Personal Data

7.1 Individuals have various rights afforded to them in respect of the information we process about them.

7.2 You must be able to recognise when someone is exercising their rights so that you can quickly refer the matter to the Data Protection Team. These rights can be exercised either in writing (e.g. in a letter or an email) or orally.

(a) Please let the Data Protection Team know if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information the CLF holds about them or their child and/or wants copies of the information we hold;

(ii) asks to withdraw any consent that they have given to use their information or information about their child (e.g. photographs);

(iii) wants the CLF to delete or erase any information;

(iv) asks the CLF to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for electronic information which they provided to the CLF to be transferred back to them or to another organisation;

(vi) wants the CLF to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the CLF newsletter or alumni events information; or

(vii) objects to how the CLF is using their information or wants the CLF to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most commonly exercised rights mentioned in section 7 above is the right to make a subject access request (SAR). Under this right individuals are entitled to request a copy of the Personal Data which the CLF holds about them (or in some cases their child) and to certain supplemental information.

8.2 SARs do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me a copy of my absence record" is a valid SAR. You must immediately let the Data Protection Team know when you receive any such requests.

8.3 Receiving a SAR is a serious matter for the CLF and involves complex legal rights. Staff must not respond to a SAR themselves unless authorised to do so.

8.4 When a SAR is made, the CLF must disclose all of the Personal Data which falls within the scope of the request - there are only very limited exemptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a SAR. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters. The CLF SAR Procedure documents the federations approach to handling requests and should be used by DP Leads when responding to a request.

9 Breaches of this Policy

9.1 Breaches of this Policy may put Data Subjects whose Personal Data is being processed at risk and carries the risk of significant civil and criminal sanctions for thee CLF and may, in some circumstances, amount to a criminal offence by the individual staff member.

9.2 Any failure to comply with any part of this Policy may lead to disciplinary action under the CLF's procedures and this action may result in dismissal for gross misconduct. If a non-member of staff breaches this Policy, they may have their contract terminated with immediate effect.

9.3 Individuals who deliberately or recklessly access, disclose, procure or retain Personal Data held by the CLF, without proper authority, may also be guilty of a criminal offence and may be reported to the Information Commissioners Office.

10 Data Protection Officer Contact Details

The DPO can be contacted using the following email address - dataprotection@clf.uk.