Cabot Learning Federation

Data Protection Policy for Staff

Date Adopted: 25 June 2020, Cabot Learning Federation

Implementation Date: 25 June 2020

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 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	

Contents

Policy Equality Impact Screening

Date of screening: **16 June 2020**						
Name of person completing screening: **John Wall**						
	Does this policy have the potential to impact on people in any of the identified groups?		What is the expected impact of this policy on any of the identified groups			Notes
	Yes	**No**	**Positive**	**Neutral**	**Negative**	
Age	X		X			The Data Protection Policy will ensure all personal data and special category personal data (e.g. race, sex, religion) is processed in accordance with GDPR and UK privacy laws.
Disability	X		X			
Gender Reassignment	X		X			
Race or Ethnicity	X		X			
Religion or Belief	X		X			
Marriage	X		X			
Pregnancy/ Maternity	X		X			
Sex	X		X			
Sexual Orientation	X		X			
Carers / in-care	X		X			
Should the policy have a Full Equalities Impact Assessment? **No**						

1 Introduction

1.1 This Policy is about your obligations under data protection legislation. 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 regarding their data - such as 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 third parties. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the CLF and will ensure that it operates successfully.

1.3 You are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy may result in disciplinary action.

1.4 The Data Protection Officer is responsible for helping you to comply with the CLF's obligations. To facilitate access to matters relating to data protection, each academy and central function 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 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 employees, 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 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 individuals. Companies and legal entities are not protected by the legislation.

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 available, regardless of the media it is recorded or held on (i.e. paper and electronic formats).

3.3 Information as simple as someone's name and address is their Personal Data.

3.4 The following are referred to as Special Categories of Personal Data in this Policy and in the Information Security Policy. You must be particularly careful when dealing with this type of Personal Data 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).

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

(a) on a computer database;
(b) in a file, such as a pupil report;
(c) a register or contract of employment;
(d) pupils' exercise books, coursework and mark books;
(e) health records; and
(f) email correspondence.

3.6 Examples of documents where Personal Data or Special Category Personal Data might be found are:

(a) a report about a child protection incident;
(b) a record about disciplinary action taken against a member of staff;
(c) photographs or CCTV (*);
(d) a tape recording of a job interview;
(e) contact details and other personal information held about pupils, parents and staff and their families;
(f) contact details of a member of the public who is enquiring about placing their child at the CLF;
(g) financial records of a parent;
(h) information on a pupil's performance; and
(i) an opinion about a parent or member of staff in an email.

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

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

3.8 Some of the conditions for processing special category and criminal offence data, set out in Schedule 1 of the Data Protection 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 General Data Protection Regulation 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 upon request and is available from the Data Protection Officer.

4 Your obligations

4.1 Personal Data must be processed fairly, lawfully and transparently.

4.1.1 What does this mean in practice?

(a) "Processing" covers virtually everything which is done with Personal Data, including collecting, using, disclosing, copying, storing and deleting it.

(b) 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 Commissioners Office (the data protection regulator).

This information is often provided in a document known as a privacy notice or privacy statement. Copies of the CLF's privacy notices can be obtained from the Data Protection Team or accessed from the CLF's pubic websites. You must familiarise yourself with the CLF's Pupil, Parent and Staff Privacy notices.

(c) 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.

(d) 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; and

(vii) to fulfil the CLF's contractual and other legal obligations.

(e) 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.

(f) 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 You must only process Personal Data for limited purposes and in an appropriate way.

4.2.1 What does this mean in practice?

(a) For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you must not use those photographs for another purpose (e.g. in the CLF's prospectus). Please see the Trust's Code of Conduct and the Data Protection frequently asked questions document for further information on the use of photographs and videos of pupils.

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 What does this mean in practice?

(a) 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.

(b) 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.

(c) 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 The Personal Data that you hold must be accurate and kept up to date.

4.4.1 What does this mean in practice?

(a) 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 You must not keep Personal Data for longer than is necessary.

4.5.1 What does this this mean in practice?

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 documents. 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 You must keep Personal Data secure.

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 New starters must complete the mandatory Data Protection 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 to the Data Protection Team immediately, who will ensure that it is captured on the CLF Breach Log and is escalated appropriately. This 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 loss of availability of personal data.

4.7 You must not transfer Personal Data outside the European Economic Area (EEA) without adequate protection.

4.7.1 What does this mean in practice?

(a) 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.

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 your Data Protection Lead.

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

5.3 **DO** encrypt emails which contain Special Category Personal Data described in paragraph 3.4 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 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 pupil recruitment event.

6 Sharing Personal Data within the CLF

6.1 This section applies when Personal Data is shared within the Trust.

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

6.3 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).

6.4 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).

6.5 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;

(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 copies of all emails you hold about me" 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 never respond to a SAR themselves unless authorised to do so.

8.4 When a SAR is made, the CLF must disclose all of that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. 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.

9 Breaches of this Policy

9.1 Breaches of this Policy may be treated as misconduct and could result in disciplinary action including, in serious cases, dismissal.

9.2 A member of staff who deliberately or recklessly accesses, discloses, procures or retains 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.