Coastal Learning PARTNERSHIP

DATA PROTECTION POLICY

This policy has undergone an Equalities Impact Assessment in line with the requirements of the Public Sector Equality Duty

Committee:	Resources Committee
Policy Ratified:	October 2025
Review Date:	October 2027

Additional School Procedure - N/A	
Committee:	
Procedure Adopted:	
Review Date:	

Contents

Section One: The Policy

1. About this policy

1.1 **Coastal Learning Partnership** (the **Partnership**) obtains, keeps and uses personal information (also referred to as data) about governors, trustees, volunteers, visitors, parents, family members and next of kin, pupils, job applicants and about current and former employees, temporary and agency workers, contractors, student teachers, volunteers and apprentices for a number of specific lawful purposes, as set out in the Partnership's Privacy Notices.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to individuals. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use, retention and deletion of all personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The Partnership's **Data Protection Officer** is responsible for informing and advising the Partnership and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Partnership's policies and procedures. Questions or comments about the content of this policy or requests for further information, should be directed to the **Data Protection Officer** on 01202 806155 or DPO@coastalpartnership.co.uk.

2. Scope

2.1 This policy applies to all processing of personal information of individuals across the Partnership.

2.2 Staff should refer to the Partnership's privacy notices and, where appropriate, to its other relevant policies including the IT and Communications Systems Policy and Freedom of Information Publication Scheme, which contain further information regarding the protection of personal information in those contexts.

2.3 We will review and update this policy periodically in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3. Definitions

3.1 "criminal records information" means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

3.2 "data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

3.3 "personal information" (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

3.4 "processing personal information" means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

3.5 "pseudonymised" means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

3.6 "sensitive personal information" (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4. Data protection principles

4.1 We will comply with the following data protection principles when processing personal information:

4.1.1 process personal information lawfully, fairly and in a transparent manner;
4.1.2 collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
4.1.3 only process personal information that is adequate, relevant and necessary for the relevant purposes;
4.1.4 keep personal information accurate and up to date, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
4.1.5 keep personal information for no longer than is necessary for the purposes for which the information is processed; and
4.1.6 take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time (if it has not already started), and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

a. that the data subject has consented to the processing;
b. that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. that the processing is necessary for compliance with a legal obligation to which the Partnership is subject;
d. that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
e. that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; and/or

f. that the processing is necessary for the purposes of legitimate interests of the Partnership or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices;

5.1.5 where sensitive personal information is processed, also identify a condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a condition for processing that information (see paragraph 7.2.2 below), and document it.

5.2 We will maintain a Data Asset Register to record our legitimate interests for requesting and using personal data, and the most appropriate basis for the lawful processing of personal data.

6. Sensitive personal information

6.1 From time to time we will need to process sensitive personal information.

6.2 We will only process sensitive personal information if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above; and
6.2.2 one of the conditions for processing sensitive personal information applies, e.g.:

a. the individual has given has given explicit consent;
b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Partnership or the individual;
c. the processing is necessary to protect the individual's vital interests, and the individual is physically incapable of giving consent;
d. processing relates to personal data which are manifestly made public by the individual;
e. the processing is necessary for the establishment, exercise or defence of legal claims; or
f. the processing is necessary for reasons of substantial public interest.

6.3 The Partnership's privacy notices set out the types of sensitive personal information that the Partnership processes, what it is used for and the lawful basis for the processing.

6.4 Before processing any sensitive personal information of a type or for a purpose not referred to in the relevant privacy notice, staff must notify the **Data Protection Officer** of the proposed processing, in order that the **Data Protection Officer** may assess whether the processing complies with the criteria noted above.

6.5 Processing of sensitive personal information of a type or for a purpose not referred to in the Partnership's data protection privacy notices will not occur until:

6.5.1 the assessment referred to in paragraph 6.4 has taken place; and

6.5.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.6 The Partnership will not carry out automated decision-making based on any individual's sensitive personal information.

6.7 Staff members are required to take particular care in relation to their processing of sensitive personal information.

6.8 All sensitive personal information must be retained and disposed of in accordance with the Partnership's specified retention periods.

Members, Trustees, Local Governors, volunteers and visitors

6.9 We process sensitive personal information only to obtain criminal records information and confirm identity.

Parents, family members and next of kin

6.10 We process contact details, medical details and details contained within support plans (which may include sensitive personal information) for the purposes of contacting parents, family members and next of kin and to protect pupil welfare and provide education.

Pupils

6.11 We process medical and health information about pupils only to protect their welfare and comply with our legal obligations. We process information relating to pupils' race or ethnicity, gender and religion or beliefs to protect pupil welfare, provide education and to comply with legal obligations.

Staff

6.12 **During the recruitment process**:

6.12.1 we do not (except where the law permits otherwise) ask for sensitive personal information e.g. relating to race and ethnic origin, trade union membership or health, during the short-listing, interview or decision-making stages;

6.12.2 if sensitive personal information not required as part of the recruitment process is volunteered, no record is kept of it and any reference to it is immediately deleted or redacted;

6.12.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and will not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.12.4 we ensure 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.12.5 we will only ask health questions once an offer of employment has been made.

6.13 Immediately following the recruitment process:

6.13.1 we will destroy copies of any documents taken to evidence identity and qualifications, except for the successful candidate.

6.14 **During employment**: we will process:

6.14.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.14.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised;

6.14.3 trade union membership information for the purposes of staff administration and administering 'check off';

6.14.4 details of family relationships (only for the purposes of identification, contacting family members or providing benefits to them or staff) which may contain sensitive personal information.

7. Criminal records information

7.1 We process criminal records information about trustees, governors, staff, volunteers and visitors to comply with our legal obligations.

7.2 We will only process criminal records information if:

7.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above; and

7.2.2 one of the conditions for processing criminal records applies, eg.:

a. the individual has given has given explicit consent;
b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Partnership or the individual;
c. processing relates to personal information which are manifestly made public by the individual;
d. the processing is necessary for the establishment, exercise or defence of legal claims; or
e. the processing is necessary for reasons of substantial public interest.

7.3 The Partnership's privacy notices describe our processing of criminal records information, what it is used for and the lawful basis for the processing.

7.4 Before processing any criminal records information for a purpose not referred to in the Partnership's data protection privacy notice, staff must notify the **Data Protection Officer** of the proposed processing, in order that the **Data Protection Officer** may assess whether the processing complies with the criteria noted above.

7.5 Processing of criminal records information for a purpose not referred to in the Partnership's privacy notices will not occur until:

7.5.1 the assessment referred to in paragraph 7.4 has taken place; and

7.5.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7.6 We will not carry out automated decision-making based on any individual's criminal records information.

7.7 All criminal records information must be retained and disposed of in accordance with the Partnership's specified retention periods.

8. Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights, we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

8.2 During the course of any DPIA, the advice of the **Data Protection Officer** and, where appropriate, the views of affected individuals, will be sought.

9. Generative AI

9.1 Generative AI is one type of AI and refers to technology that can be used to create new content using large volumes of data that have been collected from a variety of sources. ChatGPT, Microsoft Copilot and Google Gemini are examples of generative AI tools.

9.2 The CLP AI Policy defines the way in which AI can be used in Partnership schools to ensure data protection principles are upheld.

9.3 The CLP IT and Communications Systems Policy requires the filtering and monitoring of AI content.

10. Documentation and records

10.1 We will keep written records of processing activities to the extent required by data protection law, including:

10.1.1 the name and details of the Partnership (and where applicable, of other controllers, the Partnership's representative and **Data Protection Officer**);

10.1.2 the purposes of the processing;

10.1.3 a description of the categories of individuals and categories of personal data;

10.1.4 categories of recipients of personal data;

10.1.5 where relevant, details of transfers to third parties, including documentation of the transfer mechanism safeguards in place;

10.1.6 where possible, specified retention periods; and

10.1.7 where possible, a description of technical and organisational security measures.

10.2 As part of our record of processing activities we document, or link to documentation, on:

10.2.1 information required for privacy notices;

10.2.2 records of consent;

10.2.3 controller-processor contracts;

10.2.4 the location of personal information;

10.2.5 DPIAs; and

10.2.6 records of data breaches.

10.3 If we process sensitive personal information or criminal records information, we will keep written records of:

10.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

10.3.2 the lawful basis and condition for our processing; and

10.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

10.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

10.4.1 updating our information audits to find out what personal information the Partnership holds;

10.4.2 distributing questionnaires and talking to staff across the Partnership to get a more complete picture of our processing activities; and

10.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

10.5 We document our processing activities in electronic form so we can add, remove and amend information easily.

11. Privacy notice

11.1 We will issue privacy notices from time to time, informing individuals about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

11.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

12. Individual rights

12.1 Individuals have the following rights in relation to their personal information:

12.1.1 to be informed about how, why and on what basis that information is processed—see the Partnership's data protection privacy notices;

12.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;

12.1.3 to have data corrected if it is inaccurate or incomplete;

12.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

12.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the Partnership no longer needs the personal information but the individual requires the data to establish, exercise or defend a legal claim; and

12.1.6 to restrict the processing of personal information temporarily where they do not think it is accurate (and the Partnership is verifying whether it is accurate), or where they have objected to the processing (and the Partnership is considering whether its legitimate interests override the individual's interests).

12.2 Individuals wishing to exercise any of the rights in paragraphs 11.1.2 to 11.1.6, should contact the **Data Protection Officer**. Any staff member who receives a request from an individual to exercise these rights must immediately refer it to the **Data Protection Officer**.

13. Staff obligations

13.1 All staff are responsible for helping the Partnership keep their personal information up to date. They should let the HR department know if the information they have provided to the Partnership changes, for example if they move house or change details of the bank or building society account to which they are paid.

13.2 Some staff members will have access to the personal information of other employees in the course of their employment or engagement. If so, the Partnership expects them to help meet its data protection obligations to those employees.

13.3 Staff members who have access to personal information must:

13.3.1 only access the personal information that they have authority to access, and only for authorised purposes;

13.3.2 only allow individuals who are not staff to access personal information with specific authority to do so from the **Data Protection Officer**;

13.3.3 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions communicated by the Partnership);

13.3.4 not remove personal information, or devices containing personal information (or which can be used to access it), from the Partnership's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

13.3.5 not store personal information on local drives or on personal devices that are used for work purposes.

13.4 Staff should contact the **Data Protection Officer** if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

13.4.1 processing of personal information without a lawful basis for its processing or, in the case of sensitive personal information or criminal records information, without one of the conditions in paragraph 6.2.2 or 7.2.2 being met;

13.4.2 any data breach as set out in paragraph 15.1 below;

13.4.3 access to personal information without the proper authorisation;

13.4.4 personal information not kept or deleted securely;

13.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Partnership's premises without appropriate security measures being in place;

13.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

14. Information security

14.1 We will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

14.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

14.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

14.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

14.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

14.2 Where the Partnership uses external organisations to process personal information on its behalf (so that those organisations are processors as defined in applicable data protection laws), additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

14.2.1 the organisation may act only on the written instructions of the Partnership;

14.2.2 those processing the data are subject to a duty of confidence;

14.2.3 appropriate measures are taken to ensure the security of processing;

14.2.4 sub-processors are only engaged with the prior consent of the Partnership and under a written contract;

14.2.5 the organisation will assist the Partnership in providing subject access and allowing individuals to exercise their rights in relation to data protection;

14.2.6 the organisation will assist the Partnership in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

14.2.7 the organisation will delete or return all personal information to the Partnership as requested at the end of the contract; and

14.2.8 the organisation will submit to audits and inspections, provide the Partnership with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Partnership immediately if it is asked to do something infringing data protection law.

14.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the **Data Protection Officer**.

15. Storage and retention of personal information

15.1 Personal information (and sensitive personal information and criminal records information) will be kept securely in accordance with:

- The IMRS Information Management Toolkit for Academies[1]
- The CLP Finance Regulation Manual

15.2 Personal information (and sensitive personal information and criminal records information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Where there is any uncertainty, staff should consult the **Data Protection Officer**.

15.3 Personal information (and sensitive personal information and criminal records information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

16. Data breaches

16.1 A data breach may take many different forms, for example:

16.1.1 loss or theft of data or equipment on which personal information is stored;

16.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

16.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

16.1.4 human error, such as accidental deletion or alteration of data;

16.1.5 unforeseen circumstances, such as a fire or flood;

16.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

16.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

16.2 We will:

16.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

16.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

17. International transfers

17.1 The Partnership may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) in accordance with ICO guidance.[2]

[1] https://irms.org.uk/page/AcademiesToolkit

[2] https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/

17.2 If personal data is simply electronically routed through a non-EEA country but the transfer is actually from one EEA country to another EEA country, this is not a restricted transfer; this scenario applies if personal data is transferred within the EEA via a server in a non-EEA country.

17.3 Before transferring any personal data to a company or organisation based to a non-EEA country, the **Data Protection Officer** must be consulted and will ensure the transfer is appropriate and is covered by an EU Commission "adequacy decision".

18. Training

18.1 The Partnership will ensure that all staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

19. Consequences of failing to comply

19.1 The Partnership takes compliance with this policy very seriously. Failure to comply with the policy:

19.1.1 puts at risk the individuals whose personal information is being processed; and

19.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Partnership; and

19.1.3 may, in some circumstances, amount to a criminal offence by the individual.

19.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the Partnership Disciplinary Procedure, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

19.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the **Data Protection Officer**.

Section Two: Roles and Responsibilities

20. Responsibilities of the Partnership Board

20.1 The Partnership Board will:

a. Make themselves aware of the General Data Protection Regulation and the Data Protection Act 2018, and of their obligations.
b. Review and approve this policy on an annual basis.
c. Make the adequate resources available to support the work of the **Data Protection Officer**, including any necessary training.
d. Receive a summary of all data protection breaches and incidents on a termly basis.
e. Enable the **Data Protection Officer** to operate independently and ensure they are not penalised for performing their role.

21. Responsibilities of the Data Protection Officer

21.1 The **Data Protection Officer** will encourage a positive data protection culture and best practice and endeavor to ensure that all personal data is processed in compliance with the General Data Protection Regulation and the Data Protection Act 2018 through the implementation of this policy and by:

a. Providing clear data protection procedures and suitable training across the organisation to ensure the Partnership and its employees understand their data protection obligations.
b. Being available to the Partnership and its employees to give support and guidance.
c. Monitoring and auditing compliance with the policy and procedures to include:
    i. Annual audit of the Data Asset Register held by each school and the central team.
    ii. Regular monitoring of data protection information such as breaches, SARs and FOIs.
    iii. Annual reminder to cleanse the personal data retained in electronic and hard copy records.
d. Dealing with all data breaches and Subject Access Requests either personally or by working with schools – as deemed appropriate at that time.
e. Reporting data breaches to the ICO.
f. Logging all data breaches and Subject Access Requests.
g. Supplying a summary report including breaches and incidents and changes in legislation to the Trust Board on a termly basis.

22. Responsibilities of the Chief Executive Officer and the Central Senior Leadership Team

22.1 Central Senior Leaders are expected to show leadership in data protection compliance and to have regard to this policy by striving to create a culture where data protection is regarded by everyone as integral to their work. Specifically they will support the work of the **Data Protection Officer** by:

a. Making available necessary resources.
b. Through HR support and the implementation of a Partnership wide induction scheme that includes data protection awareness.
c. Involving the **Data Protection Officer** in all issues relating to the protection of personal data.
d. Facilitating an annual update of data protection awareness by all staff.
e. Ensuring that all central staff undertake required training and are aware of the Partnership's data protection procedures and that these are put into practice.
f. Ensuring that all central staff undertake an annual cleanse of electronic and hard copy data.
g. Ensuring a Data Protection Impact Assessment (**Appendix C**) is completed before the purchase of new software or systems that use personal data.
h. Providing suitable secure storage for personal and sensitive data retention.
i. Promoting clear desk principles including installing photocopiers with a secure release function and providing secure shredding machines or services.

Responsibilities of the Headteacher

22.2 The **Headteacher** is expected to show leadership in data protection compliance and to have regard to this policy by striving to create a culture where data protection is regarded by everyone as integral to their work. Specifically they will support the work of the **Data Protection Officer** by:

a. Ensuring that all school staff undertake required training and are aware of the Partnership's data protection procedures and that these are put into practice.

b. Ensuring that all school staff undertake an annual cleanse of electronic and hard copy data.
c. Ensuring a Data Protection Impact Assessment is completed before the purchase of new software or systems that use personal data.
d. Supplying a summary report to include breaches and incidents to the **Local Governing Body** using the half termly report template.
e. Promoting clear desk principles including installing photocopiers with a secure release function and providing secure shredding machines or services.

23. Responsibilities of the Local Governing Body

23.1 **Local Governing Bodies** will ensure that their school monitors and reviews its compliance against the requirements of this policy.

23.2 Receive a summary of school breaches and incidents on a termly basis.

24. Deputy Data Protection Officer

24.1 Working with the Data Protection Officer as required to cover absence and provide support.

25. Responsibilities of all staff

a. All staff are required to read and understand their legal responsibilities under this policy; Section 1 Para 12 sets out the Partnership's expectations of every individual.
b. In order to achieve these expectations, staff must attend mandatory and recommended training and demonstrate compliance with this policy.
c. Staff are responsible for seeking guidance if they are unsure about any aspect of data protection.
d. All staff should undertake an annual cleanse of electronic and hard copy data stored in personal folders and in shared folders they access to.
e. All staff must demonstrate clear desk and clear screen good practice. Keeping a clear desk and clear screen reduces the risk of data loss by ensuring personal and confidential information is not left unattended and accessible to unauthorised persons during and outside normal working hours or when the owner of the information is not there.
f. Staff only have the right of access to data during their employment. On leaving the Partnership, they must:

- Return or dispose of any pupil / staff files (either manual or computerized) and delete data held on personal devices.
- Ensure any information retained for CV purposes are anonymised.

g. All staff must ensure the security of data by:

- Only storing data on a Partnership network which is secure and password protected;
- Never storing data on a home PC or personal device;
- Never storing data on local drives;
- Keeping passwords confidential;
- Logging off or locking unattended PCs and devices;
- Keeping pupil and employee paper files in a secure place;

- Encrypting files containing personal and sensitive data if they are being emailed to an external email address and only sending using encrypted work email;
- Not leaving personal data where unauthorised people may see it;
- Disposing of data carefully and appropriately;
- Ensuring that any personal devices that have access to a Partnership network or email account has adequate security in terms of encryption or password / passcode protection and that the device automatically locks. It is the responsible of all staff to ensure the security of data or access to the Partnership network on their device;
- Ensuring that information is not held beyond the life of its purpose.

Section Three: Procedures and Guidance

26. Personal Data

26.1 The ICO explains that, "Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information."

26.2 Essentially, the name, date of birth, bank details, medical details, National Insurance Number (NINO), address, photographs / images, DBS details, next of kin – any piece of information which can identify an individual.

26.3 Some personal data is highly sensitive and classified as special category:-

a. Racial or ethnic origin
b. Political opinions
c. Religions or philosophical beliefs
d. Trade Union membership
e. Generic data
f. Biometric data
g. Health
h. Sex life
i. Sexual orientation"
j. In education the DfE recommend we include SEND, Children's Services interactions, Free School Meal Status, Pupil Premium eligibility, Safeguarding information and behaviour data

27. Data Breach

27.1 The ICO explains that "A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed."

27.2 Reporting an incident

27.2.1 All employees are responsible for ensuring data breach and information security incidents are reported immediately to the **Data Protection Officer**:

a. By doing so themselves; or
b. By ensuring that someone else does.

27.3 Breaches can be reported in the following ways:

a. By email to the **Data Protection Officer**;
b. By completion of the template at **Appendix A**;
c. By using the report form available on the CLP Intranet;
d. By logging details on purposed software (if used by the school).

27.4 For the avoidance of doubt, and to ensure no delay, all suspected breaches must be reported. In the event that it is subsequently established that a breach has not occurred then records can be updated.

27.5 The person responsible for or discovering the breach / incident should normally be the person reporting it.

27.6 Staff must not rely on a senior member of staff to decide if an incident is reportable or to report an actual or suspected incident.

27.7 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable, taking into account its severity, to ensure the breach or incident can be reported to the ICO within timescales if necessary. The timeframe for notifying the ICO is 72 hours.

27.8 The **Data Protection Officer** will ensure that breaches are recorded on the Partnership's central log.

27.9 The **Data Protection Officer** will investigate the breach by working with schools and other organisations as necessary will request additional information as required.

27.10 All staff should be aware that all data breaches will be referred to HR to ensure consistency and that any breach of the Data Protection Act could result in the Partnership's Disciplinary Procedures being instigated.

Containment and Recovery

27.11 The **Data Protection Officer** will:

27.11.1 Determine if the breach is still occurring.

27.11.2 Liaise with relevant staff to establish the severity of the breach.

27.11.3 Establish who may need to be notified as part of the initial containment and will inform the police, as appropriate.

27.11.4 Determine the suitable course of action to be taken to ensure a resolution to the incident.

27.11.5 Consider at an early stage the level of communication required with the Data Subject and other parties, and will refer to the ICO Guidance.

27.11.6 Seek advice as necessary.

Investigation

27.12 An investigation will be undertaken by the **Data Protection Officer** immediately and wherever possible within 24 hours of the breach being discovered / reported.

27.13 All actions and decisions will be logged by the **Data Protection Officer**.

27.14 The investigation will take into account the following:

- the type of data involved and its sensitivity
- the protections which are in place (e.g. encryption)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential adverse consequences on those data subject(s) and how likely they are to occur
- whether there are wider consequences to the breach

27.15 The **Data Protection Officer** will determine who needs to be notified of the breach, including: the ICO and third parties such as the police, insurers, bank or credit card companies, and trade unions.

27.16 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with an appropriate named contact officer who they can contact for further information or support in relation to what has occurred.

Communication with Data Subjects

27.17 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the law says they must be informed directly and without undue delay. In other words, this should take place as soon as possible. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. The **Data Protection Officer** will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

27.18 The **Data Protection Officer** will describe, in clear and plain language, the nature of the personal data breach and, provide at least:

- their name and contact details
- additional contact details if considered necessary
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Evaluation and response

27.19 Once the initial incident is contained, the **Data Protection Officer** will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

28. Consent

28.1 The Information Commission's Office (ICO) notes that the General Data Protection Regulation (GDPR) sets a high standard for consent, but also that it is often requested when not needed.

28.2 It is not appropriate to seek consent where there is a lawful basis to obtain, process and share personal information.

Schools should not ask for consent unless they are confident it is appropriate to do so. Where there is doubt, they should seek clarity from the

28.3 Consent must not remove the individual's rights to refuse, withdraw and rectify.

Consent or Permission

28.4 It is important to understand the difference:

- Permission – to go on a trip, take part in a school activity.
- Permission – to walk home alone.
- Consent – required if you want to use (process and retain) or share personal data, e.g, a name or a photo, for example:
    - Use of photographs and/or names on the school website.
    - Use of photographs and/or names in newsletters.
    - Giving names (and other details such as class) to outside organisations where there is no lawful basis to do so.
    - Photos for special school or offsite events – likely to be a one off, e.g, Christmas events.

Asking for consent.

28.5 Consent must be given in writing.

28.6 Verbal consent cannot be used in place of written consent, for example, to put a photograph on a website or in a newsletter a school cannot simply phone the parent.

28.7 Consent must be explicit, it must not be presumed and provision to withdrawn consent at any time must be allowed.

28.8 When requesting consent, schools must:

- Be clear the request is for consent (not permission).
- Be clear that consent can be refused without prejudice.
- Ensure a positive opt in is required, you cannot presume consent if a request is not answered.
- Ensure each consent request is listed individually; multiple consent requests must not be merged into a single request.
- Be clear about what why the data is being shared.
- Explain how the data will be stored and for how long.
- Give the right to withdraw consent at any time without prejudice.
- Ensure a record of the consent is retained.
- Ensure consent is reviewed regularly; for example, alongside the annual review of pupil data held on the school Management Information System.

28.9 Schools must use the template at **Appendix B** to gather consent on entry to the school and on review.

28.10 They may adapt the template to suite their specific arrangements, for example, not all schools use social media.

Consent for Marketing.

28.11 The review process must include a review of the use of personal data for marketing purposes. Most commonly this will be the school website or brochure.

28.12 Unless specific consent is sought and given, images should not be used on school websites or in marketing materials once a pupil has left that school.

Consent for transfers outside the EEA

28.13 **Coastal Learning Partnership** does not mandate the use of any software or system that transfers or stores data outside the EEA.

28.14 Schools should avoid the use of software and systems which does so.

28.15 Where a school decides to use software and systems which does so, they must:

a. Document their decision and the reasons for it, and
b. Seek consent for using such software or systems, and
c. Seek consent to transfer or store personal data outside the EEA.

28.16 If the data subject (or their parent/carer) does not provide both consents, or withdraws one or both consents, then the school must ensure that a pupil or member of staff is not disadvantaged in any way.

Consent to use biometric data

28.17 A Data Protection Impact Assessment must first be completed and guidance sought from the **Data Protection Officer**.

28.18 A specific request for consent will be required.

Consent and First Aid / Administering Medication

28.19 Administering first aid is not about administering medication or fluids of any kind, it is purely about making the victim safe and comfortable and seeking professional advice if the injury or condition is serious.

28.19.1 Administering first aid – we have a duty of care to pupils and this means we do **not** need to ask for permission to administer first aid. If permission is sought and refused, schools might be unable to look after a pupil in the event of an incident.[3]

28.19.2 Administering medicine - schools **do** need to ask for permission to administer medication.

29. Requests for Information

Subject Access Request (SAR)

29.1 The ICO explains that:

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

29.2 All requests for personal information must be referred to the **Data Protection Officer** at the earliest opportunity. The month for responding includes weekends and bank holidays, including Christmas and New Year so it imperative that the request is referred early. This timeframe starts from the date the request is received by the organisation, not the date it is referred to the **Data Protection Officer**.

29.3 It is the responsibility of all staff know how to recognise and refer a SAR to the **Data Protection Officer**.

29.4 Any request for personal information must be treated as a SAR, even if the requester does not use that terminology.

29.5 The **Data Protection Officer** will respond to all SARs and will work with schools and third parties to gather and collate information.

29.6 The **Data Protection Officer** is responsible for deciding what information, if any, should be redacted or withheld and will have due regard to **Keeping Children Safe in Education**[4] information sharing requirements in particular that, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about

[3] https://www.gov.uk/government/publications/first-aid-in-schools

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1007260/Keeping_children_safe_in_education_2021.pdf

sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Freedom of Information (FOI)

29.7 A FOI request is for generic information; a request that does not relate to an individual. The requester does not have to use that terminology.

29.8 Staff should be familiar with the **CLP Freedom of Information Publication Scheme**.

29.9 All FOI requests must be referred direct to the **Data Protection Officer** at the earliest opportunity. For schools, the standard response time limit is 20 school days, or 60 working days if this is shorter. This time starts from the date the request is received by the organisation, not the date it is referred to the **Data Protection Officer**.

29.10 All FOI requests must be made in writing – this could be via email. Requests can also be made via the web, or social networking sites such as Facebook or Twitter so staff who monitor these forms of communication must be alert to the possibility of a FOI request being received.

30. Data Protection Impact Assessment

30.1 The General Data Protection Regulation (GDPR) makes it a legal requirement to carry out a Data Protection Impact Assessment (DPIA) where the use of the personal information is likely to result in a high risk to the privacy of individuals, usually the use of new technologies.

30.2 **Headteachers** (or **Executive Headteacher** where appropriate) and Senior Central Leaders are responsible for ensuring the DPIA screen questions template at **Appendix C** is completed before the introduction of any new system or software.

30.3 The **Data Protection Officer** will review completion of the template and, where necessary, conduct a full Data Protection Impact Assessment in line with the ICO Guidance.

Appendix A: DATA BREACH REPORT – template

Data breaches **must** be reported immediately to the **Data Protection Officer** as outlined in Section 27 of Part Three of this policy.

Date incident was discovered:	
Date(s) of incident:	
Name of staff member who became aware of breach / incident AND name of staff member reporting breach / incident:	
Time they became aware:	
Name of staff member(s) involved:	
Name of data subjects (pupil or staff member or parent) affected – if multiple, then provide details via secure email:	
What happened? Give a brief description:	
Describe the type of data involved, what has been lost or shared.	
Brief description of any action taken at the time of discovery:	
Contact details of person reporting incident (email address, telephone number):	

Appendix B: CONSENT REQUEST – template with example consent requests

Parental consent for processing a pupil's personal data

During your child(ren)'s time at (name of school), we will gather information about them which we will use for various purposes – this information is known as personal data. Examples of personal data include:

- Images / photographs
- Names – either first name or surname
- Medical information
- Next of kin information

Our ***Privacy Notice for Pupils and Parents*** explains how we collect and use personal data and a copy is available to you on our website https://www.coastalpartnership.co.uk/ or from the office of your child's school. We will not ask you for consent to use personal data for the activities described in our Privacy Notice.

However, for some activities we must ask for your consent. For example, using pupil names or images to celebrate achievement on our website, in our school newsletter, or in other promotional material such as our prospectus.

Please read this form carefully and decide on the appropriate options for you and your child(ren).

You do not have to provide your consent, and you do not have to explain why you have chosen not to do so. We are happy to give you more information to help you make your decision and address any concerns you might have. If you choose not to provide consent for the use of your child(ren)'s personal data this will not affect your child and their time at school in any way.

A couple of points to note;

- If you do give your consent, you can choose to withdraw it at any time. Again, this will not affect your child(ren) and their time at school in any way.
- We cannot assume that you give your consent; instead if you choose not to fill out this form we will assume you have not given consent.
- We cannot accept verbal consent, it must be written.

It is therefore very important that you complete this form and return it to us. Please do let the school know if you will need any help to complete the form.

Consent on behalf of another organisation:

We cannot obtain consent on behalf of another organisation such as the Daily Echo (for example, for Reception class photographs), school photography companies or after school clubs.

For these activities, the school will contact you directly to explain the arrangements that will be made and the company themselves will ask for your consent.

I give consent for my child's image to be used on the (name of school) website	YES	NO
I give consent for my child's image to be used alongside his/her name in displays within the school premises.	YES	NO
I give consent for my child's image to be used on the Partnership website.	YES	NO
I give consent for my child's image to be used in (name of school) marketing publications such as the prospectus or open/parent evening presentations and literature.	YES	NO
I give consent for (name of school) to provide my child's image to the media in order to publicise school achievements. (NB. This only applies to images taken by the school, not to images taken by the media.)	YES	NO
I give consent for (name of school) to provide my child's name to the media in order to publicise school achievements.	YES	NO
I give consent for my child to be included in formal class and other group photographs taken by the school during teaching and learning activities.	YES	NO
I give consent for my child's image to be used on the school's social media such as Facebook / Twitter / Class Dojo / other …….	YES	NO
I give consent for my child's name and class details to be shared with the school photographer to enable individual, sibling and class photographs to be taken.	YES	NO
I give consent for my child's image to be used on internal screens/notice boards which might be visible to external visitors such as Ofsted or contractors and service providers.	YES	NO

Biometric data (*data from human characteristics*) schools to remove this section if not relevant. • (Name of school) uses biometric data to allow pupils to easily borrow books from the school library using a thumb print. • All thumb prints are stored securely (in binary) and will be destroyed as soon as your child leaves the school. • CLP and (name of school) will not collect or use biometric information about children except in accordance with the Protection of Freedoms Act 2012.		
I give consent for my child's thumb print to be used so that they can take out library books.	YES	NO

The information in this form will be obtained on first entry to the school and retained in your child(ren)'s records. We will require you to update your consent regularly along with the data we hold for your child(ren).

*If at any time, you decide to withdraw or consent you **must** inform the school office in writing and clearly identify which activity consent has been withdrawn. You can also do this by contacting the **Data Protection Officer**.*

Please sign and date before returning to the school office.

Signed:	Date:

Appendix C: DATA PROTECTION IMPACT ASSESSMENT – screening questions

These questions must be considered for all Data Subjects: pupil, staff member, volunteer, governor, trustee, contractor, consultant, etc.

If any question is answered yes, the template must be referred to the **Data Protection Officer**, together with full details of the product, for approval before procurement or implementation.

Does the proposed software or system require the collection and processing of any personal data?	YES	NO
Is any of the personal data special category data?	YES	NO
Does the proposed system monitor the movement and behaviour of data subjects?	YES	NO
Does the proposed system monitor a publicly accessible place?	YES	NO
Is the software or system a new technology? (New to the school)	YES	NO
If the answer is yes to any of the above, please provide a summary of the way in which the school will use the software or system, the advantages it will allow, and the measures that will be implemented to keep data secure and managed in accordance with the CLP Data Protection Policy:		

Data Protection Officer completion:

Software or system does not pose a significant data protection concern. Procurement / implementation may continue.	YES	NO
Further review is needed in line with the ICO guidance. Procurement and implementation must wait until this process is complete.	YES	NO