Data Protection Policy

Policy owner:	Simon Stott
Approved by:	Trust Board
Ratified by:	Risk and Audit Committee
Date:	29th January 2025
Date of next review:	31st December 2025

Contents

1 Aims

Our Trust aims to ensure that all personal data collected about staff, students, parents and carers, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and Articles of Association.

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ➢ name (including initials) ➢ identification number ➢ location data ➢ online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ➢ racial or ethnic origin ➢ political opinions ➢ religious or philosophical beliefs ➢ trade union membership ➢ genetics ➢ biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ➢ health – physical or mental ➢ sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4 The data controller

Our Trust processes personal data relating to parents and carers, students, staff, governors, visitors and other stakeholders, and therefore is a data controller.

The Trust is registered with the ICO, as legally required and will renew this annually or as required.

5 Roles and responsibilities

This policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the board of Trustees and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **Simon Stott** and is contactable via **dpo@cctrust.uk**.

5.3 Headteacher / Principal

The Headteacher / Principal within each of the Coastal Collaborative Trust (CCT) academies will act as the day-to-day representative of the data controller.

5.4 All staff

Staff are responsible for:

a. collecting, storing and processing any personal data in accordance with this policy;
b. informing the Trust of any changes to their personal data, such as a change of address;
c. contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - if they have any concerns that this policy is not being followed;
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;

- if there has been a data breach;
- whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- if they need help with any contracts or sharing personal data with third parties.

5.5 Staff Leavers

When staff leave the employment of the Trust, all permissions and access will be removed from the staff member by suspending or deleting their accounts as appropriate.

6 Data protection principles

The UK GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

a. processed lawfully, fairly and in a transparent manner;
b. collected for specified, explicit and legitimate purposes;
c. adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
d. accurate and, where necessary, kept up to date;
e. kept for no longer than is necessary for the purposes for which it is processed;
f. processed in a way that ensures it is appropriately secure.

This policy sets out how the Trust aims to comply with these principles.

7 Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

a. the data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract;
b. the data needs to be processed so that the Trust can comply with a legal obligation;
c. the data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life;
d. the data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority;
e. the data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden;
f. the individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

a. the individual (or their parent/carer when appropriate in the case of a student) has given explicit consent;
b. the data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law;
c. the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
d. the data has already been made manifestly public by the individual;
e. the data needs to be processed for the establishment, exercise or defence of legal claims;
f. the data needs to be processed for reasons of substantial public interest as defined in legislation;
g. the data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
h. the data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
i. the data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

a. the individual (or their parent/carer when appropriate in the case of a student) has given consent;
b. the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
c. the data has already been made manifestly public by the individual;
d. the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
e. the data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Further information is available in our privacy notices about the types of information the Trust holds and processes which are available on our website.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

8 Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

a. there is an issue with a student or parent/carer that puts the safety of our staff or another individual at risk;
b. we need to liaise with other agencies – we will seek consent as necessary before doing this;
c. our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law;
    - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share;
    - only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9 Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- the source of the data, if not the individual;

- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual;
- the safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- name of individual;
- correspondence address;
- contact number and email address;
- details of the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students in the trust may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our Trust may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- may ask the individual to provide forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- will provide the information free of charge;
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the student's best interests;
- would include another person's personal data that we can't reasonably anonymise, and we do not have the other person's consent, and it would be unreasonable to proceed without it;

- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

a. withdraw their consent to processing at any time;
b. ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
c. prevent use of their personal data for direct marketing;
d. object to processing that has been justified on the basis of public interest, official authority or legitimate interests;
e. challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
f. be notified of a data breach (in certain circumstances);
g. make a complaint to the ICO;
h. ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10 Parental requests to see the educational record

Parents, or those with parental responsibility, may request access to their child's educational record (which includes most information about a student) and we will aim to provide this access within 15 school days of receipt of a written request. If the request is for a copy of the educational record, the academy may charge a fee to cover the cost of supplying it.

This applies as long as the student concerned is aged under 18.

There are certain circumstances in which this may be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

11 Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school meals instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

12 CCTV

We use CCTV in various locations around the Trust sites to ensure the academies remain safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

Each academy has its own CCTV policy which operates in line with the sentiment of this policy.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to **dpo@cctrust.uk**

13 Photographs and videos

As part of the Trust's activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other

students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Uses may include:

a. within the Trust on notice boards and in CCT magazines, brochures, newsletters, etc.;
b. outside of the Trust by external agencies such as the school / college photographer, newspapers, campaigns;
c. online on our Trust's website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See the Child Protection and Safeguarding Policy of the relevant institution for more information on our use of photographs and videos.

14 Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Coastal Collaborative Trust recognises that AI has many uses to help students learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Coastal Collaborative Trust will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

15 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

a. appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
b. only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
c. completing data protection impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
d. integrating data protection into internal documents including this policy, any related policies and privacy notices;
e. regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
f. regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
g. appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply;
h. maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of the Trust and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices);
    - for all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

16 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

a. paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use;
b. papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access;
c. where personal information needs to be taken off site, staff must sign it in and out from the school office;
d. passwords that are at least 10 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites;
e. staff within the Trust will be expected to use multi-factor authentication when accessing their emails from a new device or outside of their academy;
f. encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;

g. staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see the online safety policy from the relevant institution);
h. where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

17 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

A data retention schedule of how long different data is stored is held in the Information Asset Register (IAR) for use by the Trust to ensure that data is kept only as long as is required and no longer.

18 Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches may include, but are not limited to:

- a non-anonymised dataset being published on the Trust's website, which shows the exam results of students eligible for the pupil premium;
- safeguarding information being made available to an unauthorised person;
- the theft of a Trust laptop containing non-encrypted personal data about students.

19 Training

All staff and governors are provided with data protection training as part of their induction process. These resources will be made available to staff through validated external bodies such as (but not limited to) The National College to quality and credibility of the training offered. This training will be provided by the DPO across the Trust.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Trust Board.

Appendix 1: General data protection guidelines for staff

The majority of staff will process personal data on a regular basis as part of their role in the Trust whether it is prospective, current or former students/employees, contractors, visitors etc.

A large proportion of staff will have access to and process student data in their daily work routine e.g. completing registers, marking assessments and recording grades, safeguarding, student support services, writing reports or references, or as part of a pastoral role. The Trust will ensure through registration procedures that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 2018 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- general personal details i.e. name and address;
- details about class attendance;
- coursework marks, grades and associated comments;
- pastoral notes, including matters about behaviour and discipline;

Information about a student's physical or mental health, sexual life, political or religious views is sensitive and can only be collected and processed with the students' explicit written consent, usually via the Student Services team, Additional Learning Support team, Examinations team.

Examples:

- keeping of sick notes, medical correspondence outlining conditions and treatments;
- recording information about dietary needs, for religious or health reasons, while organising for students to take part in off-site activity;
- recording information that a student is pregnant, as part of pastoral duties.

Disclosure of such information without consent is permitted only in "life or death" or safeguarding circumstances, e.g., if a student is unconscious, a teacher can tell medical staff that the student is pregnant or a Jehovah's Witness.

Sensitive information must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. All staff have a duty to make sure that they comply with the data protection principles, as set out in the Data Protection Policy.

In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- fair;
- kept securely;
- disposed of safely.

Staff must not disclose personal data to any other student, parent/carer or other person not in employment at the Trust without authorisation or agreement from the data controller, or in line with Trust policy. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with Trust policy.

The Act requires data to be kept securely in relation to both unauthorised access and loss.

All staff have a duty to maintain data security, in particular by not leaving data accessible in an unlocked office, filing cabinet or personal bags. Computer screens should not be placed where they could be easily seen by unauthorised people. Computers should be locked when left unattended. Electronic transfer of personal data cannot be considered secure. Using email or fax to transmit personal data should be treated with extreme caution. This is particularly important when sending confidential documents, such as references, to third parties outside the Trust.

Sending password documents in password protected files should be the minimum level of security applied. Before processing any personal data, all staff should consider the checklist below.

Staff checklist for recording data:

- Do you really need to record the information?
- Is the information ‘standard’ or is it ‘sensitive’(special category)?
- If it is sensitive, do you have the data subject’s express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Appendix 2: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO).

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - lost;
    - stolen;
    - destroyed;
    - altered;
    - disclosed or made available where it should not have been;
    - made available to unauthorised people.

- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher/principal and the Chair of Governors

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences

- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust central computer systems and retained in line with the data retention schedule.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Trust's awareness of the breach. As required, the DPO will set out:
    - a description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned;
        - the categories and approximate number of personal data records concerned;
    - the name and contact details of the DPO;
    - a description of the likely consequences of the personal data breach;

- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach,
  - The name and contact details of the DPO,
  - A description of the likely consequences of the personal data breach,
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - facts and cause;
  - effects;
  - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored on the Trust central computer systems and retained in line with the data retention schedule.

- The DPO and Trust Leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

- The DPO and Trust Leadership Team will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the Trust to reduce risks of future breaches.

Appendix 3: Data Protection Impact Assessment (DPIA) Template

For further information on when to complete a DPIA, visit the ICO website

Name of Controller	
Subject / title of the DPO	
Name of DPO	

Step 1: Identify the need for the DPIA.

Identify the need for the DPIA: • Explain broadly what the project aims to achieve and what type of processing this involves. You may find it helpful to refer or link to other documents, such as a project proposal. • Summarise why you identified the need for a DPIA.

Step 2: Describe the Processing

Describe the nature of the processing: • How will you collect, use, store and delete data? • What is the source of the data? • Will you be sharing the data with anyone? You might find it useful to refer to a flow diagram or other way data flows. • What types of processing identified as likely high risk are involved?

Describe the scope of the processing: • What is the nature of the data, and does it include special category or criminal offence data? • How much data will you be collecting and using? How often? • How long will you keep it? • How many individuals are affected? • What geographical area does it cover?

Describe the context of the processing: • What is the nature of your relationship with the individuals? • How much control will they have? • Would they expect you to use their data in this way? • Do they include children or other vulnerable groups? • Are there prior concerns over this type of processing or security flaws?

- Is it novel in any way?
- What is the current state of technology in this area?
- Are there any current issues of public concern that you should factor in?
- Are you signed up to any approved code of conduct?

Describe the purposes of the processing:

- What do you want to achieve?
- What is the intended effect on individuals?
- What are the benefits of the processing – for you, and more broadly**?**

Step 3: Consultation Process

Consider how to consult relevant stakeholders: • Describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? • Do you need to ask your processors to assist? • Do you plan to consult information security experts, or any other experts?

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: • What is your lawful basis for processing? • Does the processing achieve your purpose? • Is there another way to achieve the same outcome? • How will you prevent function creep? • How will you ensure data quality and data minimisation? • What information will you give individuals? • How will you help to support their rights? • What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and Assess Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** (Remote, Possible or Probable)	**Severity of harm** (Minimal, Significant, Severe)	**Overall Risk** (Low, Medium or High)
1.			
2.			
3.			

**add extra rows if needed*

Step 6: Identify Measures to Reduce Risk

Identify additional measures you can take to reduce or eliminate the risks identified as medium or high risks in Step 5				
Risk Number	**Options to reduce or eliminate risk**	**Effect on risk** (Eliminated, Reduced, Accepted)	**Residual risk** (Low, Medium, High)	**Measure Approved** (Yes / No)

Step 7: Sign Off and Record Outcomes

Item	Name / Position / Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by		If accepting any residual high risk, consult the ICO before going ahead.
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.


Coastal
Collaborative Trust