



Compass Eko Trust

Data Protection Policy



Monitoring, evaluation and review

The DPO is responsible for monitoring and reviewing this policy. The DPO may also get input from appropriate persons at Compass Eko Trust.

This policy will be reviewed and updated if necessary in line with any legislative changes which affect Compass Eko Trust’s practices. Otherwise, this policy will be reviewed every 3 years and shared with all academies.

The Board of Trustees will assess the implementation and effectiveness of this policy. The policy will be promoted and implemented throughout all Trust schools.

This Policy will be reviewed by the Trust Board on a three-yearly cycle.

Adherence to the policy will be monitored by the Local School Committee.

Policy adopted:	Spring Term 2026
Other related policies:	Online Safety Freedom of Information Policy and Publication Scheme Data Retention Use of Personal Devices Remote learning
Next Review:	Spring Term 2029

Contents

Monitoring, evaluation and review	1
Contents	3
1. Contacts:	4
2. Aims.....	5
3. Legislation and guidance.....	6
4. Definitions	6
5. The Data Controller.....	7
6. Roles and responsibilities	7
7. Data protection principles	9
7.1 Collecting personal data	9
7.1.1 Lawfulness, fairness and transparency	10
7.1.2 Limitation, minimisation and accuracy.....	10
7.2 Sharing personal data	11
8. Subject access requests (SARs) and other rights of individuals	11
8.1 Subject access requests	12
8.2 Responding to subject access requests	12
8.3 Children, subject access requests and age of consent	14
9. CCTV.....	14
10. Photographs and videos	15
11. Data protection by design and default.....	15
12. Data security and storage of records	16
13. Disposal of records	18
14. Personal data breaches	18
15. Training.....	19
Appendix 1: Subject Access Request Procedure.....	19
Appendix 2: Personal Data Breach Procedure.....	23
Appendix 3: Data Protection Impact Assessment (DPIA) Procedure.....	30
Data Protection Impact Assessment Form	34

1. Contacts:

Data Protection Officer (DPO) for the Trust is the DPO Centre, and our direct contact is Katie Handshaw, contactable via advice@dpocentre.com

For an interim period there is a separate DPO arrangement for schools that were part of the Eko Trust. The initial contact for these schools is: DPO@theeducationspace.co.uk

Data Compliance Officer: Director of IT and Head of Governance contactable via dpo@compassps.uk

Local Data Officer (LDO): School contact, usually the Office Lead/School Operations Manager, contactable via the school email address or school website

This policy applies to all members of The Compass Partnership of Schools (“the Trust”) trading as Compass Eko Trust. For the purposes of this policy, the term “staff” means all members of staff within the Trust, including permanent, fixed-term and temporary staff. It also refers to governors, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust. This policy also applies to all members of staff employed by any of the Trust’s subsidiary companies.

All contractors and agents acting for or on behalf of the Trust will be made aware of this policy.

2. Aims

Our Trust aims to ensure that all personal data collected about staff, children, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

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

The Compass Partnership of Schools trading as Compass Eko Trust is a single legal entity, therefore references to ‘CompassEko Trust’ in this policy should be considered as inclusive of its academies.

3. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. 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 code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

Personal data - Any information relating to an identified, or identifiable, living individual. This may include the individual's:

- Name (including initials);
- National Insurance 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 - categories of personal data which are more sensitive and so need 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, facial appearance, retina and iris patterns), where used for identification purposes, such as to log into a device;
- 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.

5. The Data Controller

The Compass Partnership of Schools trading as Compass Eko Trust processes personal data relating to parents, children, staff, governors, visitors and others, and is, therefore, a data controller. The Compass Partnership of Schools is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

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

Compass Eko Trust Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust and its academies comply with all relevant data protection obligations.

Data Protection Officer

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 Trust Business Committee and, where relevant, report to the Trust Board with their advice and recommendations on academy data protection issues.

Our legal DPO is the DPO Centre, and our direct named contact is Katie Handshaw, contactable via advice@dpocentre.com

The named contact for legacy Eko schools is Rachel Roberts, contactable via DPO@theeducationspace.co.uk

The relevant contact as above is also the first point of contact for individuals whose data the Trust processes. The DPO Centre will be the contact for the ICO.

Data Compliance Officer

This responsibility is shared by the Head of Governance and the Director of IT and Digital Communications, who will act as the representative of the DPO on a day-to-day basis. They will coordinate with the Data Protection Officer on specific data protection matters.

Local Data Officer

Each academy will be supported by a nominated Local Data Officer (LDO) who will coordinate with the Data Compliance Officer on specific data protection matters and will be the primary point of contact for each school. This will usually be the Office Lead/School Operations Manager or School Business Manager, but can be delegated to another member of staff who has sufficient knowledge of data practices.

All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing their school office of any changes to their personal data, such as a change of address.
- Contacting their Local Data Officer (LDO) in the following circumstances:
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - If they are engaging with any contracts or sharing personal data with third parties;
 - If they need to rely on or capture consent.
 - If there has been a data breach;
- Contacting their Data Compliance Officer (DCO) in the following circumstances:
 - If there has been a data breach and the LDO is not available;
 - 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 draft a privacy notice, deal with data protection rights invoked by an individual (such as a Subject Access Request), or transfer personal data outside the European Economic Area.
- Contacting the relevant DPO in the following circumstances:
 - If there has been a serious data breach and the LDO or DCO is unavailable;
 - If they need to deal with data protection rights invoked by an individual (such as a Subject Access Request) and the LDO or DCO is unavailable.

7. Data protection principles

The UK GDPR is based on data protection principles that the Trust must comply with. The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

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

7.1 Collecting personal data

7.1.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful basis' (legal reasons) to do so under data protection law:

- 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;
- The data needs to be processed so that The Compass Partnership of Schools can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life;
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions;
- The data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden);

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This will normally be in the form of a Privacy Notice.

7.1.2 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.
- 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 Data Retention Policy.

7.2 Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we may need to seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and children – for example, health care professionals. When doing this, we will:
 - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us;
- We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
 - The prevention or detection of crime and/or fraud;
 - The apprehension or prosecution of offenders;

- o The assessment or collection of tax owed to HMRC;
- o In connection with legal proceedings;
- o Where the disclosure is required to satisfy our safeguarding obligations;
- o Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

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 children or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8. Subject access requests (SARs) and other rights of individuals

8.1 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;
- 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.

SARs must be submitted to the DPO. In the event of a verbal request being made, the employee to which the request was made should ensure that an electronic report is made. Requests should include:

- Name of individual;
- Correspondence address;
- Contact number and email address;
- Details of the information requested.

If staff identify a subject access request, they must immediately report it to the Data Compliance Officer and forward details of the request to dpo@compassps.uk

The SAR will be responded to following the Trust's SAR Procedure (see Appendix 1)

8.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual to confirm the request was made;
- Will respond without delay and within 1 calendar month of receipt of the request;
- 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 calendar month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual;
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Is contained in adoption or parental order records;
- Is given to a court in proceedings concerning the child.
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
- A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

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

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- 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 at dpo@compassps.uk.

8.3 Children, subject access requests and age of consent

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

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of data processing or a subject access request. Therefore, parental consent is sufficient, and subject access requests from parents or carers of children who are under the age of 13 may be granted without the express permission of the child.

By contrast, children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of data processing or a subject access request. Therefore, subject access requests from parents or carers of children who are 13 and over may not be granted without the express permission of the child, and the consent of the child will be sought if consent is required for the legal processing of the child's data.

A child's ability to understand their rights in respect of the above will always be judged on a case-by-case basis, especially if the child in question has significant special educational needs. Therefore, at the Trust's SEND schools, for each cohort over the age of 13, the head teacher will assess if there are any children with a sufficient level of understanding to consent to the processing of their data or for their data to be included in a SAR from their parent. For all other children consent will remain with the parent/carer.

9. CCTV

We use CCTV in various locations to ensure our children and staff remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

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 academy CCTV systems should be directed to the individual academies themselves. For further information regarding our use of CCTV, please refer to our CCTV Policy.

10. Photographs and videos

As part of our regular activities, we may take photographs and record videos of individuals within the Trust.

We will obtain written consent from parents/carers for photographs and videos to be taken of children for communication, marketing and promotional materials, even if the subject(s) seems willing to do it. We will clearly explain how the photograph and/or video will be used to both the parent/carer and child.

Uses may include:

- Within each school on notice boards and in school newsletters, brochures, etc;
- Online on the Trust's websites 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 i.e. a child's full name will not appear next to their photograph.

External agencies, such as health care providers, newspapers, researchers, etc. who wish to take photos or videos of our children within any academy should seek consent directly with the parent/carer of the child, with the procedure facilitated and monitored by the Trust. We will ensure that the external agency is conforming to data protection regulations and ensure that the parent/carer understands what they are consenting to.

11. 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:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- 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;
- Completing privacy impact assessments where the 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);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Performing a Data Protection Impact Assessment before the commencement of any new service or project that involves the processing or sharing of personal information (See Appendix 3).
- 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;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the Trust and relevant DPO arrangement 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept securely under lock and key when not in use
- Papers containing confidential personal data must not be left unattended on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access, unless required for medical or SEND purposes. Medical or SEND records will be locked away overnight.
- It is the responsibility of all staff to ensure the integrity and security of any personal data they are processing. This includes ensuring that no one is able to view any papers

they are working on or see their computer screen. Privacy screens can be provided on request.

- Digital personal data will only be stored on platforms that guarantee the data is held in the UK.
- For legacy schools from the Compass Partnership of Schools this will be limited to Microsoft 365 Tenancy (SharePoint, OneDrive, etc.), cloud-based MIS (Bromcom), MyConcern or on the Trust's on-site secure storage servers.
- For legacy schools from Eko Trust this will be the Eko Trust's Google Workspace tenancy, Bromcom, CPOMs, Evolve/Medical Tracker or on the Trust's on-site secure storage servers.
- Digital personal data will not be stored on any other service the Trust uses for day-to-day activities, such as Google's G-Suite or Apple's iCloud.
- On-site servers will be kept in a secure, locked location away from general access, with sufficient off-site backup. Servers should be protected by an uninterruptable power supply (UPS).
- Complex passwords must be used to access the Trust's cloud-based systems, computers, laptops and other electronic devices. A password can be classed as complex when it is at least 8 characters long, contains uppercase and lowercase letters and numbers and at least one special character. Words such as family members' names, dates of birth or any other easily guessable word or phrase should not be used.
- Login details should not be divulged to anyone. It will be the responsibility of each member of staff to ensure the integrity and security of their login details for each system. Failure to do so may result in disciplinary action.
- All senior staff members' accounts will be protected by multi-factor authentication wherever possible.
- All devices will be protected by Trust-approved antivirus and malware protection solutions.
- Personal information should be kept out of email mailboxes as much as possible. On receiving an email containing personal data, the email or attachment should be saved elsewhere and the email deleted.
- If personal data has to be sent via email, the data should be secured within an encrypted, password protected file or archive.
- Personal data should not be sent internally via email. Alternative sharing methods, such as SharePoint, Google Drive or Office 365 Teams should be used.
- Staff or governors who access personal information on their personal devices are expected to follow the procedures set out in the Use of Personal Devices Policy
- 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 by the third party.
- Where data needs to be sent to a third party, we must ensure the method of transfer is secure. If data must be sent through the post, for example for secondary transfer, Royal Mail secure special delivery, or an equivalent for an alternative postal service that ensures the location of the package at all times and sufficient insurance.

13. 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 securely and permanently 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. See the Trust Data Retention Policy for more information on our retention periods.

14. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, we will follow the relevant data breach procedure – see appendix 2.

When appropriate, if the breach is deemed to have impacted on the data subject's rights or freedoms, we will report the data breach to the ICO within 72 hours, as advised by the Trust DPO. In the event of a breach that may be reportable taking place at a legacy Eko school, advice and guidance will be sought from the Education Space DPO in the first instance who will in turn liaise with the DPO Centre. Such breaches in an educational context may include, but are not limited to:

- A non-anonymised data set being lost, or published accidentally;
- Safeguarding information being made available to an unauthorised person;
- The theft of a Trust laptop containing non-encrypted personal data about a child;
- A letter containing personal data being sent to the wrong address;
- A document or device containing sensitive data being left unattended where it is likely that it was viewed by an unauthorised person.

15. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional learning, if changes to legislation, guidance or the Trust's processes make it necessary, and also as general refresher training.

Appendix 1: Subject Access Request Procedure

Access to information

Current and former pupils and staff, or any other person which we hold data for can request access to the information/data held on them by making a subject access request.

Schools will respond to Subject Access Requests themselves, liaising with the Data Compliance Officer and the relevant Data Protection Officer. The procedure should be conducted by the School's Local Data Officer reporting to the head teacher.

All subject access requests for data held by our schools should be forwarded to dpo@compassps.uk

All requests will be dealt with within one calendar month, as per the UK GDPR.

This procedure does not apply when a parent is exercising their rights under The Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) (Pupil Information Regulations), which grant parents of pupils at maintained schools the right to access their children's educational records and set out when such requests may be refused.

Subject Access Request Procedure

1. Requests for information may be made in any format, which may include email or a verbal request. If the initial request does not clearly identify the information required, then further enquiries will be made. The Data Protection Officer, Data Compliance Officer and the school's Local Data Officer should be informed immediately, and a copy of the request sent to dpo@compassps.uk.
2. The identity of the requestor must be reasonably established before the disclosure of any information from a minimum of two identifying documents, and checks should also be carried out regarding proof of relationship to the child. Acceptable forms of ID include, but are not limited to:
 - passport
 - driving licence
 - utility bills with the current address
 - Birth / Marriage certificate
 - P45 / P60
 - Credit Card or Mortgage statement
3. For any child aged 13 or over, the head teacher will assess if the child has a sufficient level of understanding to consent to their data being included in the SAR. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child. It is important to recognise that children are entitled to privacy and that there may be a duty of confidentiality owed to them which must be adhered to. If it is the child themselves that has made the subject access request, before discussing with a parent, the school will ask the child whether they object to their parents becoming aware of this request and will abide by the child's wishes unless there is an overriding public interest reason why that should not be the case. Before proceeding with informing a parent in these circumstances, advice of the Data Compliance Officer should be sought.
4. The school will not charge for the provision of information, dependent upon the following:
 - If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
 - A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.
5. The response time for Subject Access Requests, once officially received, is one calendar month. However, the one calendar month will not commence until after receipt of fees or clarification of any further information sought. The school should respond as quickly as is reasonably possible.
 6. All information held by the school on the Data Subject should be considered for inclusion in the SAR, including emails, reports, records covering safeguarding, SEN, behaviour, attainment, staff performance and discipline. The UK GDPR allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.
 7. There is no right to access for information kept individually by teachers or other staff in notebooks or teacher mark books. These include such records generated and held electronically.
 8. For information related to the Data Subject that has been provided by a third party, for example, another pupil, parent, member of the family, the school must consider whether the information held was given in circumstances where an expectation of confidentiality has arisen. The school must also consider whether or not the information is already known to the pupil or parent concerned. If information is in the public domain, and/or the school is satisfied that the information is already known, then it may be disclosed. Information provided by the Police, Local Authority, Health Care professional or another school, may also have been provided to the school in the expectation that it will be held confidentially. Where the information is a medical record made by an external health care professional, the consent of that professional must be sought before it may be released.
 9. Any information which, it is believed may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
 10. If there are concerns over the disclosure of information, then additional advice should be sought from the Data Compliance Officer in the first instance.
 11. If any part of the information to be disclosed compromises the data security of another individual, for example, if another pupil is named on a report, then the name or any other identifiable data should be redacted (information blacked out/removed). Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why. If redaction is not possible, then consent of the individual, or their parent/carer must be sought.
 12. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
 13. Information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then recorded special delivery mail must be used.

Complaints

Complaints about the handling of a subject access request should be made directly to the relevant Data Protection Officer.

Complaints about the above procedures should be made in accordance with the Trust's complaints process.

Complaints which are not appropriate to be dealt with through the Trust's Complaints Policy can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

For information regarding subject access requests see

<https://ico.org.uk/for-the-public/personal-information>.

Appendix 2: Personal Data Breach Procedure

What is a Data Breach

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 and this unavailability has a significant negative effect on individuals.

Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it – this could be verbally, in writing or electronically.
- Theft / loss of a confidential paper
- Sending personal data to an incorrect recipient .e.g. the sending of an email to the wrong address or the sending of a pupil report to the wrong parent.
- Sending a text message containing personal data to all parents by mistake.
- Writing down your password and leaving it on display or somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially (e.g. leaving it on a printer).
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person.
- Computer infected by a Virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on School ICT equipment.
- Accessing a computer database using someone else's authorisation (e.g. using someone else's user ID and password to access Bromcom).
- Changes to information or data or system hardware, firmware, or software characteristics without the school's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- Open public discussion of data protected and confidential information including discussion of employees, pupils or parents within the Trust.
- The unauthorised use of a system for the processing or storage of data by any person.

Data Breach Procedure

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the school's Local Data Officer or the Data Compliance Officer. You should preserve all evidence relating to the potential Personal Data Breach.

On finding or causing a breach, or potential breach, the Local Data Officer or the Data Compliance Officer will inform the Data Protection Officer and the relevant head teacher and take immediate remedial steps to mitigate and remedy the breach that has occurred. All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed. Breaches involving particularly risky or sensitive information must be acted upon swiftly, e.g. safeguarding or health information.

The DPO will provide advice on the immediate steps to be taken, investigate the report, and determine whether a breach has occurred.

The Local Data Officer will complete a Data Breach Report form (see below) and store it securely, alongside any other relevant documentation. A copy will be sent to the DPO.

The Data Compliance Officer will carry out an internet search to check that the information has not been made public, if it has; we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

The Data Compliance Officer will assess the risk to individuals, based on the severity and likelihood of potential or actual impact. If the risk is high, the Local Data Officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- 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

Reporting the breach to the Information Commissioner's Office - The [Trust](#) Data Protection Officer will consider whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people’s rights and freedoms, the Trust DPO must notify the ICO within 72 hours of the personal data breach being identified.

Each academy will maintain a record of all data breaches which occur, regardless of their severity or need to report to the ICO.

Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website within 72 hours. 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. 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.

Review and Planning

The DPO, DCO, LDO and head teacher/ executive head teacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible. A report of data protection breaches and information security incidents will be presented to the Compass Eko Board of Trustees.

Breach Example:

Health records for a child have been sent to the wrong email address.

The person who sent the email will immediately inform their Local Data Officer, who will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The LDO will then inform the DPO, DCO and head teacher. The LDO will begin to complete the data breach report form. The LDO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request. These responses will be kept secure alongside the report. The LDO will discuss with the Data Compliance Officer or the Data Protection Officer if the Data Subject (s) parents/carers should be informed. In this case, as it is a special category of information, the LDO will notify the parents/carers. The DPO will then determine if the ICO should be informed.

Reporting Information Security Weaknesses

All staff are responsible for ensuring that our data is held securely. Security events or potential security weaknesses, for example a cupboard containing data being left unlocked, or out of date virus protection, must be reported immediately to the Data Compliance Officer. A Data Protection Impact Assessment must be carried out, and mitigation action including implementation timeframes, should be undertaken.

Staff must not attempt to prove a security weakness as such action may be considered to be misuse of information assets.

Weaknesses in a third party application or service provider must also be reported. The provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded and reported.

Security events can include:

- Access violations, e.g. password sharing
- Breaches of physical security, e.g. broken locks
- Non-compliance with policies
- Repeated lock out of user accounts
- Malicious software (virus infections)
- Unscheduled shutdowns, system errors or overloads
- Documents left unattended on desks

Security weaknesses can include:

- Inadequate firewall or antivirus protection

- Unlocked cupboards
- Weak passwords
- Human error
- Computer monitors being routinely overlooked by unauthorised individuals.

Compass Eko Trust

Data Breach Report Form

NB: For use by Legacy Compass Schools only

Legacy Eko schools to report via this link [here](#)

Name of School	
Date of breach	
Data Subject (e.g. name of pupil/member of staff whose data has compromised)	
Name of Person(s) Involved in Breach (e.g. anyone who has had contact with the data leading up to and after the breach)	
Details of data lost/disclosed (please give as much information as possible regarding the incident)	
Measures taken to limit impact	
Was Data Recovered?	<input type="checkbox"/> Yes (please tick) <input type="checkbox"/> No
Parties Informed of Breach (Including data subject/guardians and any authorities)	
Is the breach considered a risk to the Data Subject's rights or freedoms? – DPO to advise	<input type="checkbox"/> Yes (please tick) <input type="checkbox"/> No

If yes to the above, has the ICO been informed within 72 hours? – DPO to advise	<input type="checkbox"/> Yes (please tick) <input type="checkbox"/> No		
Any Further Action Taken			

Name of Local Data Officer (Person dealing with breach)			
Signature of Local Data Officer		Date	
Signature of head teacher		Date	

Appendix 3: Data Protection Impact Assessment (DPIA) Procedure

A DPIA is a way to systematically and comprehensively analyse data processing and help identify and minimise data protection risks. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to indicate that all risks have been eradicated. But it helps to document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA. A DPIA is not a one-off exercise. It is an ongoing process that is subject to regular review.

When do we need to perform a DPIA?

We must perform a DPIA before we begin any type of processing that is “likely to result in a high risk”. This means that although we have not yet assessed the actual level of risk, we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says we must do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

- When considering if your processing is likely to result in high risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

The ICO also requires us to do a DPIA if we plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.
- You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

Data Protection Impact Assessment Form

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Please refer to the Data Protection Policy while completing this assessment.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it 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 data with anyone? You might find it useful to refer to a flow diagram or other way of describing 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 data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected?

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 or certification scheme (once any have been approved)?

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 with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's 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 actually 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	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/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 kept under review by:		The DPO should also review ongoing compliance with DPIA