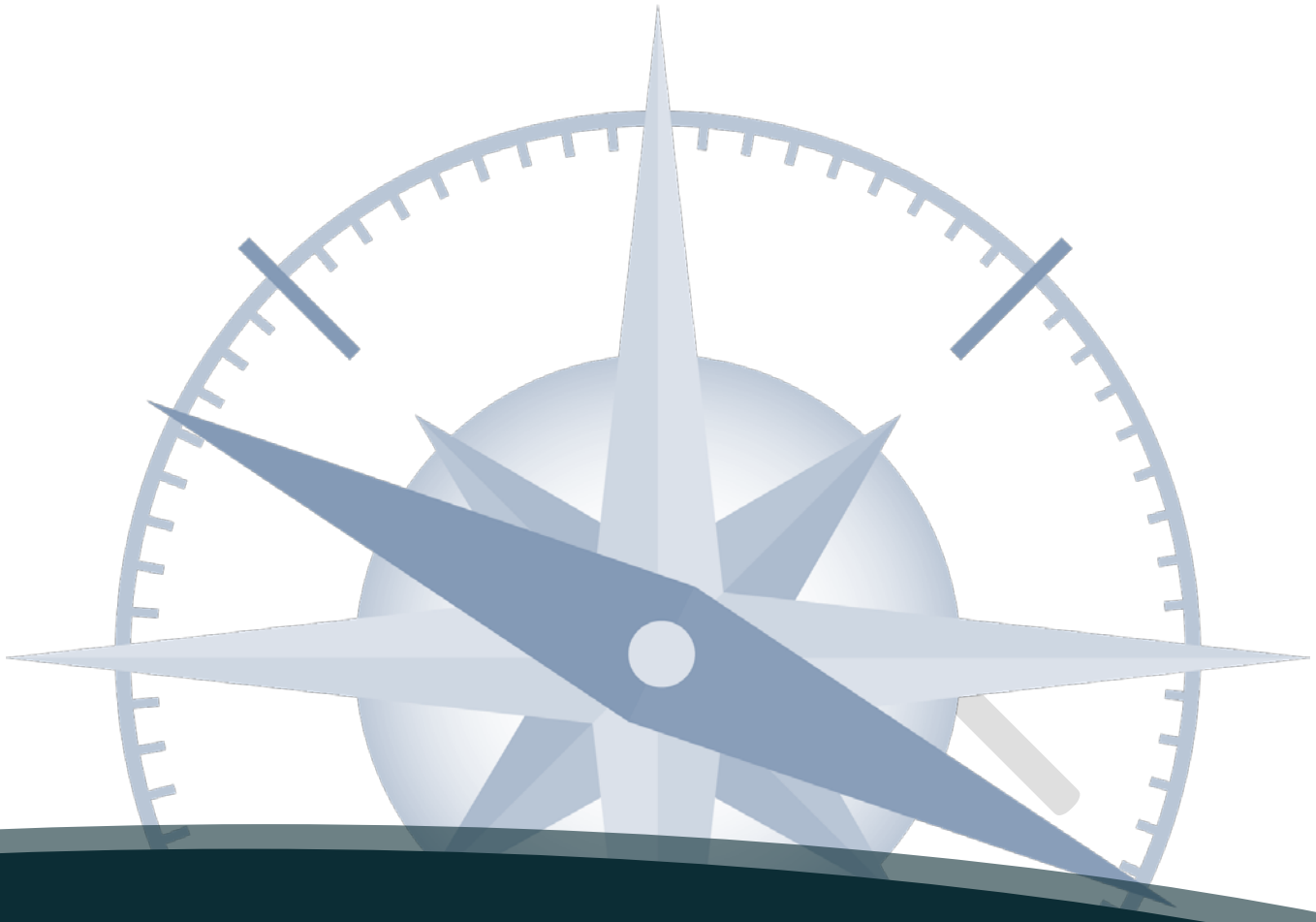

Data Protection Policy

Encorporating the Subject Access Request and Data Breach Procedures

THE COMPASS PARTNERSHIP OF SCHOOLS

This policy applies to all members of The Compass Partnership of Schools ("the 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.

Aims

Our Trust aims to ensure that all personal data collected about staff, childs, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and provisions of 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 is a single legal entity, therefore references to 'The Compass Partnership of Schools' in this policy should be considered as inclusive of its academies.

Legislation and guidance

This policy meets the requirements of the 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.

Definitions

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 - 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 of 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.

The Data Controller

The Compass Partnership of Schools processes personal data relating to parents, childs, 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.

Roles and responsibilities

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

The Compass Partnership of Schools Board of Trustees
The Board of Trustees has overall responsibility for ensuring that The Compass Partnership of Schools 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 Resources Committee and, where relevant, report to the Trust Board their advice and recommendations on academy data protection issues.
The DPO is also the first point of contact for individuals whose data The Compass Partnership of Schools processes, and for the ICO. Our DPO is Nathalie Fitzgerald and is contactable via dpo@compassps.uk

Data Compliance Officer
The Trust Head of IT and Digital Communications will act as the representative of the data controller 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.

All Staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing the Trust head 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.
- Contacting their Data Compliance Officer (DCO) 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.
- Contacting the DPO in the following circumstances:
    - If there has been a data breach;
    - 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, or

transfer personal data outside the European Economic Area.

Data protection principles

The GDPR is based on data protection principles that The Compass Partnership of Schools 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 Compass Partnership of Schools aims to comply with these principles.

Collecting personal data

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 Compass Partnership of Schools can fulfil a contract with the individual, or the individual has asked The Compass Partnership of Schools 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 Compass Partnership of Schools, 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 Compass Partnership of Schools 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 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 is normally be in the form of a Privacy Notice.

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 The Compass Partnership of Schools Data Retention Policy.

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 childs – for example, health care professionals. When doing this, we will:
    - Only appoint suppliers or contractors which 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;
    - The assessment or collection of tax owed to HMRC;
    - In connection with legal proceedings;

- Where the disclosure is required to satisfy our safeguarding obligations;
- 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 childs 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.

Subject access requests and other rights of individuals

Subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that The Compass Partnership of Schools 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.

Subject access requests must be submitted in writing, either by letter or email to the DPO. They 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 Compass Partnership of Schools SAR Procedure (see Appendix 1)

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 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 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.

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 either be unable to understand their rights and the implications of 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 childs 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 childs 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 Willow Dene School, 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 at Willow Dene School, consent will remain with the parent/carer.

Biometric recognition systems

In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use childs' biometric data as part of an automated biometric recognition system (for example, childs use biometric to receive academy dinners 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 Compass Partnership of Schools 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 childs have the right to choose not to use The Compass Partnership of Schools's biometric system(s). We will provide alternative means of accessing the relevant services for those children.

Parents/carers and childs can object to participation in The Compass Partnership of Schools's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a child 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 child's parent(s)/carer(s).

Where staff members or other adults use The Compass Partnership of Schools'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 Compass Partnership of Schools will delete any relevant data already captured.

CCTV

We use CCTV in various locations to ensure they remains 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 academy themselves.

Photographs and videos

As part of our regular activities, we may take photographs and record videos of individuals within The Compass Partnership of Schools.

We will obtain written consent from parents/carers, or children aged 18 and over or who are vulnerable in any way, 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 Compass Partnership of Schools 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.

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 Compass Partnership of Schools' 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;
- 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 Compass Partnership of Schools 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, 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.

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 staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- 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 The Compass Partnership of School's Office 365 Tenancy (SharePoint, OneDrive, etc.), cloud-based MIS (SIMS) or on the Trust's secure storage servers.
- 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 Compass Partnership of Schools' 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 letters and numbers and at least one special character.
- 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 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 or Office 365 Teams should be used.
- Staff or governors who access personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment. Personal data should be accessed directly on the cloud storage platform and not downloaded to the personal device. They will consent to their personal devices being inspected at any time to ensure this is being adhered to.
- 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.

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 Compass Partnership of Schools'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 The Compass Partnership of Schools Data Retention Policy for more information on our retention periods.

Personal data breaches

The Compass Partnership of Schools 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 The Compass Partnership of Schools data breach procedure – see appendix 2.

When appropriate, if the breach is deemed to have impacted on the data subjects rights or freedoms, we will report the data breach to the ICO within 72 hours, as advised by the DPO. 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 achild;
- 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.

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 Compass Partnership of Schools's processes make it necessary, and also as general refresher training.

Monitoring arrangements

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

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect The Compass Partnership of Schools's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with all academies.

Links with other policies

This data protection policy is part of the The Compass Partnership of Schools Information Governance Framework and is linked to our:
Online Safety Policy;
Freedom of Information Policy and Publication Scheme;
Data Retention Policy.

Appendix 1

The Compass Partnership of Schools
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 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 30 calendar days.

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 grants 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 must be made in writing, which includes email. 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 30 calendar days. However, the 30 calendar days 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 school be considered for inclusion in the SAR, including emails, reports, records covering safeguarding, SEN, behaviour, attainment, staff performance and discipline. The General Data Protection Regulation (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 health record made by a 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 Trust Data Protection Officer, Nathalie Fitzgerald, who can be contacted at dpo@compassps.uk.

Complaints about the above procedures should be made to the Chair of the Governing Body for the relevant school.

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

Appendix 2

The Compass Partnership of Schools
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 SIMS).
- 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 Hawkswood Group/ school.
- 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 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's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the personal data breach being identified.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

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 Headteacher/ Executive Headteacher 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 Board of Trustees.

Breach Example:

Health records for a child has 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. Theses 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 to ensure that our data is held securely. Security events or potential security weaknesses, for example a cupboard containing data being left unlocked, or out of data virus protection, must be reported immediately to the Data Compliance Officer. A risk 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.

THE COMPASS PARTNERSHIP OF SCHOOLS

Data Breach Report Form

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	
Measures taken to limit impact	
Was Data Recovered?	☐ Yes (please tick) ☐ 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	☐ Yes (please tick) ☐ No
If yes to the above, has the ICO been informed within 72 hours? – DPO to advise	☐ Yes (please tick) ☐ 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	