Data Protection Policy

Ensuring Compliance

With GDPR and the Data Protection Act 2018

Cidari | All Academies | Internal

Version 3.0 Published 5th April 2021

Table of Contents

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (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.

2. Legislation and guidance

This policy meets the requirements of the GDPR 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 also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right to access their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

all personal data, regardless of whether it is in paper or electronic format.

3. Definitions

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individuals:

	• Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of the 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.
The Trust	Cidari Multi Academy Trust (Cidari Education Ltd) including any of its member Academies.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our Trust processes personal data relating to parents, pupils, staff, governors, trustees, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

5.1. Trust Board is responsible for:

● The Trust Board of Trustees (through its Local Governing Committees) has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

5.2. Data Protecon Officer is responsible for:

● 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 governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.
● The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.
● Our DPO is Matt McIver and is contactable at dpo@cidari.co.uk

5.3. Chief Execuve and Headteachers are responsible for:

● The CEO and Headteachers act as the representative of the data controller on a day-to-day basis.

5.4. All Staff are responsible for:

● Collecting, storing and processing any personal data in accordance with this policy ● Informing the Trust of any changes to their personal data, such as a change of address ● Contacting the DPO in the following circumstances:
○ With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
○ If they have any concerns that this policy is not being followed
○ If they are unsure whether or not they have a lawful basis to use personal data in a particular way
○ If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
○ If there has been a data breach
○ Whenever they are engaging in a new activity that may affect the privacy rights of individuals
○ If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

6.1. The GDPR is based on data protection principles that our Trust must comply with. The principles say 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. Processing personal data

7.1. Lawfulness, fairness and transparency

- We will only process general category personal data where we have one or more 'lawful bases' (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 Trust 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 individual (or their parent/carer when appropriate in the case of a pupil) 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:-

- The individual (or their parent/carer where appropriate in the case of a pupil) has given their explicit consent
- The data has been "manifestly made public by the Data Subject". For example, by posting it on Twitter
- To carry out rights and obligations under employment law. For example, processing to ensure the health and safety of stakeholders, TUPE, etc.
- To establish, exercise or defend legal claims
- To protect the vital interests of a staff member or other person, where they are legally or physically incapable of giving consent

- For the assessment of a person's working capacity either on the basis of UK law or

under contract with a health professional, such as an external occupational health provider

- Certain special category data may only be processed if the data controller has a lawful basis under both Article 6 and Article 9 of the GDPR, and one associated Data Protection Act (2018) Schedule 1 condition. The 'Appropriate Policy Document' at Appendix 1 details how the Trust complies with this requirement.

7.2. Data Relang to Criminal Proceedings/Convicons or Child Protecon/Safeguarding Issues.

- We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where processing is necessary to carry out our obligations and provided we do so in line with data protection legislation.
- This information is not routinely collected and is only likely to be processed by the Trust in specific circumstances. For example, as a result of an appointment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during the period of employment of service with the Trust; if a child protection issue arises; or if a parent/carer is involved in a criminal matter.
- Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police.
- Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data secure.
- Whenever we first collect personal data directly from individuals, we will:-
- provide them with the relevant information required by data protection law via a Privacy Notice
- only collect personal data for specified, explicit and legitimate reasons.
- If we want to use personal data for reasons other than those given when we first obtained the data, we will inform the individuals concerned before we do so and seek consent where necessary.
- If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as the sole basis for processing, we will obtain parental consent in all instances (except for online counselling and preventive services).

7.3. Limitaon, minimisaon and accuracy

- We will only process personal data when our obligations and duties require us to. We will not collect excessive data and we will ensure any personal data collected is adequate and relevant for the intended purposes.
- When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data - see Data Retention Policy and Schedule for further guidance.

- We will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards.
- We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

7.4. Examples of When the Academy Might Process Personal Data

- The Trust must process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement). For example:
- Making decisions about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working.
- To maintain our single central record and to comply with our general safeguarding obligations.
- To provide information on our website about our employees.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Liaising with your pension provider.
- Administering the contract entered into with you.
- Operating as a Trust, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data.
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Responding to complaints or investigations from stakeholders or our regulators.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Providing references to prospective employers.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.

- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To review and better understand employee retention and attrition rates.
- In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion.
- To maintain and promote equality in the workplace.
- To comply with requirements of the Southwark Diocesan Board of Education to share personal data about employees to the extent that they require it to fulfil their functions
- To receive advice from external advisors and consultants.
- To liaise with regulatory bodies, such as the NCTL, the Department for Education, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters.
- For any other reason which the Trust is obliged to give notice of, from time to time.

7.5. How Personal Data Should be Processed on Behalf of the Trust

- Everyone who works for, or on behalf of, the Trust and its constituent Academies has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy its associated policies and procedures.
- Staff should only access personal data covered by this policy if it is required for the work they do for, or on behalf of the Trust and only if authorised to do so.
- Staff should only use the data for the specified lawful purpose for which it was obtained.
- Staff should not share personal data informally.
- Staff should keep personal data secure and not share it with unauthorised people. • Staff should regularly review and update personal data. This includes telling the Trust if their own contact details change.
- Staff should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- Staff should use strong passwords.
- Staff should lock computer screens when not at their desks.
- Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this. • Staff should not save personal data to their own computers or other electronic devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with GDPR and the Data Protection Act (2018) and in consultation with the Data Controllers representative and the DPO.

- Staff should not leave paper containing personal data lying about on desks. Storage drawers and filing cabinets should be locked.
- Staff should not take personal data away from Academy premises without authorisation from their line-manager.
- Where possible paper copies of personal data should be shredded and disposed of securely after transfer to the appropriate electronic systems. Where hard copy data is retained it should be done so securely.
- Staff should ask for help from the Data Protection Officer/ if they are unsure about data protection or if they notice any areas of data protection or security that can improve upon.
- Any deliberate or negligent breach of this policy may result in disciplinary action being taken under the Trust's Disciplinary Procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request (see below). Such conduct would also amount to gross misconduct under the Trust's Disciplinary procedure and could result in dismissal.

8. Sharing Personal Data

8.1. We will not normally share personal data with anyone else unless statutory or contractual obligations require us to do so, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

8.2. Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. 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

8.3. We are required, by law, to pass certain information to specified external bodies, such as the Department for Education, Ofsted, etc. 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 any emergency that affects any of our pupils or staff.

9. Transfer of Data Outside The European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

We will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA.

This means that we cannot transfer any personal data outside the EEA unless:

- The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the GDPR applies (including if an individual explicitly consents to the proposed transfer).

All staff must comply with the Trust's guidelines on transferring data outside of the EEA. **10.**

Subject Access Requests And Other Rights Of Individuals 10.1.

Subject access requests (SARs)

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

A SAR may be made in writing or verbally, through traditional channels of communication or Social Media.

If a SAR request is received it should forward it immediately to the Data Controller's

representative who will liaise with the Data Protection Officer and coordinate a response.

A SAR does not have to contain the words 'Subject Access Request'. Any communication, whether written or verbal, that requests access to personal data should be treated as a

possible SAR until proved otherwise. Refer to the Subject Access Request Procedure (Appendix 3, below), for further information.

A form is available to staff, Governors, parents and other stakeholders who wish to make a SAR in relation to their own personal data. Use of the form is not compulsory.

The Trust or constituent Academy must accept a SAR in any written or verbal form. We may, however, contact the requester for further information if necessary. As a minimum a SAR request should include:

- The full legal name of the requester and the data subject if different, as in the case of a pupil
- Correspondence address
- Contact number and email address
- Details of the information requested

10.2. Children and subject access requests

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

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

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

10.3. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification if we are not confident about the requester's identity or their entitlement to the data
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- 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 the information if it:

- Might cause serious harm to the physical or mental health of the pupil 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.

Should we refuse a request, we will explain to the individual why the request is refused and notify them that they have the right to complain to the ICO.

10.4. Other data protecon rights of the individual

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

- Withdraw their consent to the 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 the 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 Trust. If staff receive

such a request, they must immediately forward it to the DPO.

11. Parental Requests to See The Educational Record

Parents, or those with parental responsibility, can request to have access to their child's educational record (which includes most information about a pupil).

Such requests should be made directly to the relevant Academy. Details of the process and charges can be found on the local Academy website.

12. CCTV

We use CCTV in various locations around Trust sites to ensure it 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 the CCTV system should be directed to the Trust Head of Operations.

CCTV images are subject to the same levels of protection from unauthorised assess as any other personal data.

Requests to view CCTV images should be recorded on the appropriate form and retained together with a Viewing Log. See the ***CCTV Viewing Procedure*** in Appendix 4 for further information

13. Photographs and Videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

- Within both Academy and wider Trust notice boards and publications magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers,

campaigns
- Online on Academy and wider Trust websites.
- Trust and Academy social media channels including but not limited to Twitter, Facebook, Instagram, LinkedIn.

Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include:

- On a pupil database to identify pupils
- On care plans or allergy lists to identify pupils

A record of images used on social media, websites and in marketing campaigns will be maintained to assist with swiftly locating images of individuals.

Consent to use images on may be refused or withdrawn at any time.

If consent is withdrawn, we will delete the photograph and/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.

Please see our ***Social Media Policy*** for further information on use and guidance for social media.

See our ***Safeguarding and Child Protection Policies*** for more information on our use of photographs and videos.

14. 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 (see section 6)
- Completing privacy impact assessments where the Trusts 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 our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal ***Record of Processing Activity*** (RoPA), detailing of the categories of data processed, categories of data subjects, the purpose and lawful basis for processing, details of any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. 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 under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off-site, staff must sign it in and out from the Academy office as per agreed conventions
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust networks, computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

We may also use a third party to safely dispose of records on the Trusts behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Records of all disposal events will be maintained in accordance with the Data Retention Policy and Schedule

17. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a breach or a suspected data breach, we will follow the procedure set out in Appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an Academy context may include, but are not limited to:

- access by an unauthorised third party (including hacking, successful phishing attempts, or other access to data by unauthorised individuals.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient, or not inserting groups of email addresses in the BCC field.
- deliberate or accidental alteration of, or deletion of personal data.
- loss of availability of personal data.
- A non-anonymised dataset being published on the Academy website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft or loss of a Trust laptop, or other computing device containing non-encrypted personal data about pupils, staff or other stakeholders.

18. Training

All staff, governors, volunteers and Trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, in response to security incidents or data breaches and where changes to legislation, guidance or the Trusts processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated on a biennial basis unless interim reviews are required as a result of an amendment to Data Protection legislation or guidance, or any internal concerns resulting from policy violations or data breaches

The Data Controller's Representative, together with the Data Protection Officer will ensure the Trust and its constituent Academies comply with this policy by, among other things, reviewing records, policies, procedures and Data Protection Audits

At every review, the policy will be shared with the Schools Governing body and the Trustees if substantial changes are made.

20. Links With Other Policies and Documents

This data protection policy is linked to our:

- Appropriate Policy Document
- Data Security Policy and Procedure
- Subject Access Request Policy and Procedure
- Privacy Notices
- CCTV Policy and Access Procedure
- Freedom of information publication scheme
- Freedom of Information Policy and Procedure
- Charging & remissions policies
- Data Retention Policy and Schedule
- Secure desk policy
- Social media policy
- Internet and Email Acceptable Use Policy
- Confidential Waste Policy (pending)
- Disciplinary Policy and Procedure