Data protection policy

City of London Academies Trust

Approved by:	Board of Trustees	**Date:**	19 April 2018
Next review due by:	April 2019 or before if appropriate		

Contents

1. Aims

The City of London Academies Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the ~~expected~~ provisions of the Data Protection Act 2018 (DPA 2018) ~~as set out in the Data Protection Bill~~.

This policy applies to all personal data, regardless of whether it is in paper or electronic format, and seeks to provide guidance to Trust staff, trustees and governors on the handling of personal data.~~.~~

2. Legislation and guidance

This policy meets the requirements of the GDPR and the ~~expected~~ provisions of the DPA 2018. It is based on guidance and best practice 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 main and supplementary funding agreements and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs

	• Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing 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.

4. The data controller

The 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

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

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust and each Academy complies with all relevant data protection obligations.

5.2 Data protection officer

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

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

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

The DPO shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assist with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assist the Trust with maintenance of records;
- Monitoring and advice relating to FOI and other information requests;
- Co-operation with, and acting as the contact point for the Information Commissioner's Office, who are the supervisory authority in respect of all data protection matters;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training of Trust staff and workforce.

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

Our DPO is ~~James England and is~~Data Protection Education contactable via:

Telephone: 0800 0862018

Email: dpo@dataprotection.education

5.3 Academy representative

Each Academy in the Trust will have a nominated person acting as the representative of the data controller on a day-to-day basis within that Academy. The representative is responsible for the implementation of this Data Protection Policy within their Academy.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and the policies listed in Section 20.
- 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

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

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate and, where necessary, kept up to date;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary**;
- **Processed in a manner that ensures appropriate security of the personal data**
- **Must NOT be transferred to people or organisations situated in other countries without adequate protection.**

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Trust will only process personal data where it has one of 6 '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 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 pupil) has freely given clear **consent**. If an Academy offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, the Academy will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

~~*Primary Academies*~~

~~If an Academy offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, the Academy will get parental consent (except for online counselling and preventive services).~~

~~*Secondary and Post-16 Academies*~~

~~If an Academy offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, the Academy will get parental consent where the pupil is under 13 (except for online counselling and preventive services).~~

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

7.2 Limitation, minimisation and accuracy

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

If the Trust wants to use personal data for reasons other than those given when the data was first obtained, the Trust will inform the individuals concerned before doing 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 Records Retention Policy.

8. Sharing personal data

The Trust may share personal data when there is a lawful basis to do so as defined above in Section 7.1.

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

- There is an issue with a pupil or parent/carer that puts the safety of Trust staff at risk
- The Trust needs to liaise with other agencies – the Trust will seek consent as necessary before doing this
- Trust suppliers or contractors need data to enable the Trust to provide services to its staff and pupils – for example, IT companies. When doing this, the Trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with current 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 the Trust

The Trust will also share personal data with law enforcement and government bodies where it is 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 the Trust's safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- 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, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO. Subject access requests should be managed in accordance with the Trust Subject Access Request procedure. ~~.~~

9.2 Children and subject access requests

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

~~*Primary Academies*~~

~~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 below the age of 12 at our 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.~~

~~*Secondary and Post-16 academies*~~

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 aged 12 and above at our 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.

9.3 Responding to subject access requests

When responding to requests, the Trust:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual the Trust will comply within 3 months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within 1 month, and explain why the extension is necessary

The Trust will not disclose 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, the Trust 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 the Trust refuses a request, the individual will be told why, and told they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when the Trust is collecting their data about how the Trust uses and processes it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust 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.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record of their child in the Trust academies. However, each academy will consider any parental requests on an individual basis and may choose to provide the information requested subject to the wider requirements of this Data Protection policy and the General Data Protection Regulation.

11. Biometric recognition systems

Where the Trust uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use ~~finger prints~~fingerprints to receive lunches instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012. (In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18).

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

Parents/carers and pupils have the right to choose not to use the Trust's biometric systems. The Trust will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and the Trust will make sure that any relevant data already captured is deleted.

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

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

12. CCTV

The Trust uses CCTV in various locations around the Trust Academy sites to ensure the sites remain safe. The Trust will adhere to the ICO's code of practice for the use of CCTV.

The Trust does not need to ask individuals' permission to use CCTV but makes 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 main office at the relevant Academy.

13. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our Academies using only academy-owned devices and equipment.~~s.~~

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

~~*Secondary and Post-16 Academies:* The Academy will 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 parental consent is needed, the Academy will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent is not needed, the Academy will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within an Academy on notice boards and in magazines, brochures, newsletters, etc.
- Outside of an Academy by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust and/or Academy websites or social media pages

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

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

14. Data protection by design and default

The organisation takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

The Trust will put measures in place to show that it has integrated data protection into all of its 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 Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process). The Trust will complete an assessment of any such proposed processing, in consultation with the DPO, and will use a template document which ensures that all relevant matters are considered.
-
- 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 the Trust's privacy measures and make sure it is compliant
- Maintaining records of the Trust's processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Trust and DPO and all information the Trust is required to share about how their personal data is used and processed (via Trust privacy notices)
    - For all personal data that the Trust holds, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why the data is being stored, retention periods and how the data is being kept secure

15. Data security and storage of records

The Trust 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 relevant Academy office
- Use of strong passwords to access Trust 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 (see our ICT Acceptable Use Policies)

- Where the Trust needs to share personal data with a third party, the Trust will 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 the Trust cannot or does not need to rectify or update it.

For example, paper-based records will be shredded or incinerated, and electronic files overwritten or deleted. The Trust may also use a third party to safely dispose of records on the its behalf. If it does so, the Trust will require the third party to provide sufficient guarantees that it complies with data protection law.

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 suspected data breach, the Trust will follow the procedure set out in appendix 1.

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

- A non-anonymised dataset being published on the Trust or an 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 of a Trust laptop containing non-encrypted personal data about pupils

18. 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 development, where changes to legislation, guidance or the Trust's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

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 our Trust's practice. Otherwise, or from then on, this policy will be reviewed **annually**.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Records Retention Policy
- ICT Acceptable Use Policies

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the principal/headteacher, academy representative and the chair of governors of the relevant Academy, the Trust Chief Financial Officer and Chief Executive Officer and the Chair of the Trust Board.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out 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.
- 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. Documented decisions are stored in a password protected file on the Trust's computer system.
- 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO 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
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored in a password protected file on the Trust's computer system.
- The DPO, academy representative and principal/headteacher of the relevant academy will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO 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 DPO will ensure the Trust receives a written response from all the individuals who received the data, confirming that they have complied with this request

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

EXAMPLES OF DATA BREACHES

- *Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;*
- *A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes;*
- *Personal data disclosed orally in error in a meeting or over the phone – including "blogging" where information is obtained by deceiving The Organisation, or where information has been disclosed without confirming the true identity of the requester;*
- *Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;*
- *Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;*
- *Sensitive information left on a photocopier or on a desk in County Council premises;*
- *Unauthorised alteration or deletion of information;*
- *Not storing personal and confidential information securely;*
- *Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;*
- *Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.*
- *school*

Examples of Breaches caused by IT Security Incidents:

- *Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls;*
- *Hacking or phishing attacks and related suspicious activity;*
- *Virus or malware attacks and related suspicious activity;*
- *ICT infrastructure-generated suspicious activity;*
- *Divulging a password to another user without authority.*

APPENDIX 2. DEALING WITH SUBJECT ACCESS REQUESTS

What must the school do?	Why?	How?
We must be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter of the request for clarity.	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request; If the request is for non-personal information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR). NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).
If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The GDPR stipulates that SARs must be completed within one month of the request – but in reality, as soon as possible.	Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.

If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows: All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely The Organisation will meet its statutory deadlines. BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.	If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018. The request can be for either hard copy or any type of electronic information including email traffic i.e. the time and information that an email is sent. The request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.	It is in the public interest that requests are identified and dealt with as quickly as possible.	Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.