DUDLEY ACADEMIES TRUST

GDPR/ Data Protection Policy

Issue number:	002
Responsible:	Compliance & Safeguarding Officer
Approved by:	Board of Trustees
Date:	May 2020
Review date:	May 2022

Contents

Introduction

Statutory Obligations

It is the intention of Dudley Academies Trust to fulfil its obligations under the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018). It is the aim of the Trust to ensure that all staff are properly trained, fully informed of their obligations under the GDPR and are aware of their personal liabilities. Any employee deliberately acting outside of their recognised responsibilities may be subject to the Trust's disciplinary procedures.

Individuals whose information is held and processed by the Trust can be assured that their personal data will be treated with due care. This policy document applies only to information covered by the GDPR and relevant legislation impacting upon it. This policy will be a dynamic document that will be updated periodically according to the laws as set out by the European Union. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act (2000)
- The Education (Student Information) (England) Regulations 2015
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Protection of Freedoms Act 2012
- The Academy Standards and Framework Act 1998

The policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include an 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 fingertips, 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 an 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.

Before processing 'special category' information we will identify and document the lawful basis for processing this information. We will only process special categories of personal information in certain situations.

This will be done in accordance with Data Protection Law and other related government legislation.

Scope

An essential activity within [**insert name of Academy**] is the requirement to gather and process information about its learners, staff, parents/carers and other individuals who have contact with the academy, in order to enable it to provide education and other associated functions.

In addition, there may be a legal requirement to collect and use information to ensure that the academy complies with its statutory obligations.

[**Insert name of Academy**] and the Local Advisory Committee, acting as custodians of personal data, recognise their moral duty to ensure that it is handled properly and confidentially at all times, irrespective of whether it is held on paper of by electronic means. This covers the whole lifecycle, including:

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data;
- The disposal/destruction of personal data

[**Insert name of Academy**] and the Local Advisory Committee also has a responsibility to ensure the data subjects have appropriate access to details regarding personal information relating to them.

Objectives

By following and maintaining strict safeguards and controls, [**insert name of Academy**) and the Local Advisory Committee will:

- Acknowledge the rights of individuals to whom personal data relate, and ensure that these rights may be exercised in accordance with Data Protection Law;
- Ensure that individuals are fully informed about the collection and use of personal data through the publication of the academy's Privacy Notice;
- Collect and process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Ensure that adequate steps are taken to ensure the accuracy and currency of data;

- Ensure that for all personal data, appropriate security measures are taken – both technically and organisationally – to protect against damage, loss or abuse;
- Ensure that the movement of personal data is done in a lawful way – both inside and outside the organisation and that suitable safeguards exist at all times.

In order to support these objectives, the academy and the Local Advisory Committee will:

- Have a **"Senior Information Risk Owner"** (SIRO) to ensure that there is accountability and that Information Risk is recognised at a Senior Level;
- Have a designated **"Data Protection Officer**" (DPO) to meet the academy's obligations under Article 37 of GDPR
- Ensure that all activities that relate to the processing of personal data have appropriate safeguards and controls in place to ensure information security and compliance with the Data Protection Law;
- Ensure that all contracts and service level agreements between **[insert name of Academy]** and external third parties (including contract staff – where personal data is processed) include the relevant Data Protection clauses and appropriate Organisational and Technological measures will be put in place to safeguard the data;
- Ensure that all staff (**including volunteer staff**) acting on **[insert name of Academy]** behalf understand their responsibilities regarding information security under the Act, and that they receive the appropriate training/instruction and supervision so that they carry these duties out effectively and consistently and are given access to personal information that is appropriate to the duties they undertake;
- Ensure that all third parties acting on **[insert name of Academy]** behalf are given access to personal information that is appropriate to the duties they undertake and no more;
- Ensure that any requests for access to personal data are handled courteously, promptly and appropriately, ensuring that either the data subject or their authorised representative have a legitimate right to access under Data Protection Law, that their request is valid, and that information provided is clear and unambiguous;
- Ensure that all staff are aware of the Data Protection Policy and Guidance;
- Review this policy and the safeguards and controls that relate to it annually to ensure that they are still relevant, efficient and effective.
- This Policy and Procedure and the Subject Access Information material will be made available in other formats where necessary.

Roles and Responsibilities

Compliance & Safeguarding Officer

The Local Advisory Committee has overall responsibility for ensuring that our academy complies with all relevant data protection obligations. A GDPR lead will be appointed from the Local Advisory Committee to liaise with Dudley Academies Trust Compliance and Safeguarding Officer on all matters relating to data protection. The Local Advisory Committee will also be

updated, as a standing agenda item at each meeting, on any data breaches or major changes in policy.

YourIG Service

YourIG DPO Service (Data Protection Officer) will inform and advise the Trust and its employees about their obligations to comply with the GDPR and other Data Protection laws. They will also monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members. The appointed DPO will have professional knowledge and expertise of data protection law, particularly that in relation to Trusts.

Sufficient resources will be provided to the Trust to ensure that they are able to meet their GDPR obligations. The Compliance and Safeguarding Officer will report to the highest level of management at the Trust, which is the Chief Executive Officer (CEO). Each individual Academy will have a Data Protection Representative who will lead on Data Protection issues locally and will be advised and work together with the Trusts Compliance and Safeguarding Officer and YourIG DPO Service.

The Trusts Compliance and Safeguarding Officer is the first point of contact for individuals whose data the academy processes, and for the ICO:

Dudley Academies Trust – Compliance and Safeguarding Officer
Mrs Rebecca Meacham
Dudley Academies Trust
Priory Villa, 3a Ednam Road
Dudley,
DY11HL

Email: rebecca.meacham@dudleycol.ac.uk

The contact details of the individual Academy Data Protection Representatives can be found on the academy's Privacy Notice.

All Staff Members Employed by Dudley Academies Trust

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy of any changes to their personal data, such as 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

Collecting Personal Data

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' to do so under data protection law:

- The data needs to be processed so that the academy can fulfil a contract with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy can comply with a legal obligation The data needs to be processed to ensure that vital interests of the individual, e.g. to protect a life
- The data needs to be processed so that the academy, 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 academy 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 Learner) has freely given clear consent.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. These reasons will be disclosed to the individual upon data collection and can also be found in the respective academy's Privacy Notice. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Data Retention policy.

Consent

Some data that we collect is subject to active consent by the data subject. Where consent is required, it must be a positive indication. Where consent is given, a record will be kept documenting how and when consent was given. Consent for the use of this data can be withdrawn by the individual at any time.

Sharing Personal Data

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

- There is an issue with a Learner or parent/carer that puts the safety of our staff at risk
- It is necessary to liaise with other agencies – where necessary we will seek consent
- Our suppliers or contractors need data to enable us to provide services to our staff and Learners – 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; in respect of all current suppliers or contractors, contact has been made by Dudley Academies Trust to ensure compliance with GDPR
- 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, but not exhaustive of:

- 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 Learners 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. For an up to date list of who we share data with, see each respective academy's Privacy Notice.

Subject Access Requests/Subject Information Requests and other Rights of Individuals

Subject Access/Subject Information Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy holds about them. There are a few exceptions to this rule, such as information held for child protection or crime detection/prevention purposes, but most individuals will be able to have a copy of the information held on 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.

Any codes used in the record will be fully explained and any inaccurate, out of date, irrelevant or excessive information will be dealt with accordingly. Any Person/s who wish to access their data are to direct queries to the Trusts Compliance and Safeguarding Officer.

Subject access requests must be submitted in writing; either by letter or email to the Trusts Compliance and Safeguarding Officer. They should include:

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

Children and Subject Access Requests

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

Children aged 13 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 learners at our academy may not be granted without the express permission of the learner. This is not a rule and a learner's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- 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

We will not disclose information if it:

- Might cause harm to the physical or mental health of the Learner 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 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 disclose to the individual.

Other Data Protection Rights of the Individual

In accordance with 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:

- Challenge processing which has been justified on the basis of public interest;
- 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;
- 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);
- Withdraw permission to processing of data that has been subject to consent at any time.

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.

Parental Requests to see the Educational Record

Responsibility of the Trust

The Trust is responsible for a learner's educational record being made available for their parent to see, free of charge, within 15 academy days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this must be provided to them, also within 15 academy days of that request being received.

The governing body can charge a fee for the copy, but if they do this it must not be more than the cost of supply. The educational record will include the curricular record but also other information about the learner that may be kept by the academy, such as details of behaviour and family background, the definition is given below.

Please follow this link to the ICO's website https://ico.org.uk/ which provides further detailed guidance on a range of topics including individual's rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.

The Educational Record

A learner's educational record is comprised of any record of information, other than information which is processed by a teacher solely for the teacher's own use, which:

- Is processed by or on behalf of the governing body of, or a teacher at, any academy maintained by a local authority (LA) and any special academy not so maintained;
- Relates to any person who is or has been a learner at any such academy; and originates from or was supplied by or on behalf of;
- Any employee of the Dudley Academies Trust which maintains the Academy (or former academy) attended by the learner to whom the record relates;
- Where the academy is a voluntary aided, foundation or foundation special academy or a special academy not maintained by an LA, any teacher or other employee at the academy or at the learner's former academy (including any educational psychologist engaged by the governing body under a contract for services),
- The learner to whom the record relates or a parent of that learner. Additionally, it includes:
    - Any statement of special educational needs held in respect of the learner;
    - Any Personal Education Plan (PEP) held in respect of the learner. The PEP is the document initiated by children's social services when a child is taken into care and maintained by the child's academy, which provides a record of educational needs, objectives and progress and achievements.

- Information covered by the definition above falls within a variety of categories, including child protection records, records where a child has a statement of SEN and records regarding exclusions.

Biometric Recognition Systems

Learners

Where we use Learner's biometric data as part of an automated biometric recognition system, for example in the case of paying for academy lunch, we will comply with the Protection of Freedoms Act 2012.

Parents/carers will be notified before any additional biometric recognition system is put in place or before their child first takes part in it. The academy 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 Learners have the right to choose not to use the academy's biometric system. Alternative means of accessing the relevant system will be provided for those Learners.

Parents/carers and Learners can object to participation in the academy's biometric recognition system(s), or withdraw consent, at any time; we will ensure that any relevant data already captured is deleted.

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

Staff Members

Where staff members or other adults use the academy'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 academy will delete any relevant data already captured.

CCTV

We do not need to ask individual's permission to use these cameras, but we make it clear where individuals are being recorded (https://ico.org.uk/media/1542/cctv-code-of-practice.pdf). Security cameras, both stationary and on security personnel, are clearly visible and where necessary accompanied by prominent signs explaining that the cameras are in use.

Any enquiries about the CCTV system should be directed to the trusts Compliance and Safeguarding Officer. A separate policy on the use of CCTV can be found on the academy website.

Photographs and Videos

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

We will obtain written consent from parents/carers, for photographs and videos to be taken of Learners 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 learner. Where we don't need parental consent, we will clearly explain to the Learner how the photograph and/or video will be used.

Uses of photographs and videos include:

- Within academy on notice boards and in academy magazines, brochures, newsletters, etc. (consent not required)
- Outside of the academy by external agencies such as the academy photographer, newspapers, campaigns (through consent)
- Online on our academy website or social media pages (through consent)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See our photograph policy for more information on our use of photographs and videos.

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 academy'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)
- 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 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 academy 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 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 highly confidential personal information needs to be taken off site, appropriate measures to ensure its safety will be taken
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices.
- Staff and Learners are reminded to change their passwords at regular intervals and should not reuse passwords from other sites
- Encryption software is used to protect portable devices
- Staff, Learners or governors will not store personal information on their personal devices and rather use the academy's Office 365 environment
- 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

Disposal of Confidential Waste Paper

Identifying Confidential Waste

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

Defining confidential waste is key to ensure documentation is being disposed of correctly. Confidential waste is defined as any personal information that can be used to identify

individuals, including their name, address, contact numbers or any sensitive data. Examples of confidential documentation that needs disposing of correctly includes:

- Learner records;
- Staff records;
- Payroll information;
- Medical information;
- Invoices and quotes;
- Memo, notes, emails, letters.

Compliance

To ensure the trust is fully compliant with the Data Protection Act, confidential information will need destroying in a secure way by a responsible person or company. BS EN 15173: Secure Destruction of Confidential Material provides key conditions that must be adhered to fully comply to the Data Protection Act, such as:

- The screening of personnel;
- Confirmed premises security;
- The safe collection, retainment and transfer of sensitive information;
- Control over the destruction of confidential data;
- Traceability of the destruction process.

Disposing of paper information (Non-Confidential)

Dispose of unwanted paper documents that do not contain any confidential information, should be disposed of using your academie's normal procedure. Where possible if your academyl has a recycling scheme in place, this should be done through this method.

Disposing of paper information (Confidential)

Each academy site will be provided with a secure method to dispose of confidential waste in the form of lockable confidential waste bins. These will be located around each academy site that is convenient to staff areas with the highest amount of confidential waste.

Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction:

Only authorised site personnel or an approved contractor should handle the waste

Destruction is to take place off site by a specialised contractor. The waste must be escorted off site they will need to provide destruction certificates. These will be provided to the Site Manager who will keep a record of these on site.

Responsibilities and Accountabilities

Compliance with this procedure is mandatory for all staff working for or on behalf of the Trust including learners, volunteers and private contractors. They are also responsible for being aware of, and complying with the disposal waste procedures in the use in the locality in which they work.

Any breach of this procedure should be reported directly to the Trust's Compliance and Safeguarding Officer and the Principal of the specific academy.

Disposal of Electronic Information

Personal Data Breaches

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

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

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

- A non-anonymised dataset being published on the academy website which shows the exam results of Learners eligible for the Learner premium
- Safeguarding information being made available to an unauthorised person
- The theft of an academy laptop containing non-encrypted personal data about Learners

Training

- All staff and Local Advisory Committee members 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 academy's processes make it necessary.

Appendix 1: Personal Data Breach Procedure

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

We 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. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Compliance and Safeguarding Officer (CSO) who will report the breach to the Data Protection Officer (DPO)
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or
  - Made available where it should not have been o Made available to unauthorised people
- The CSO will alert the Principal and the Trust Board.
- The CSO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- 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 o 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 on the academy's compliance 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 CSO 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).