

Data Protection Policy

CEO:	Chris Moore
Written by:	Cook Lawyers
Written/Adopted:	July 2026
Ratified by Trustees:	(insert date)
Next Review:	July 2028

Contents

1. Aims
 2. Legislation and guidance
 3. Definitions
 4. The data controller
 5. Roles and responsibilities
 6. Data protection principles
 7. Collecting personal data
 8. Sharing personal data
 9. Subject Access requests and rights of individuals
 10. Parental requests to see the educational record
 11. CCTV
 12. Photographs and videos
 13. Data protection by design and default
 14. Data security and storage of records
 15. Disposal of records
 16. Personal data breaches
 17. Data protection complaints
 18. Training
 19. Monitoring arrangements
 20. Links with other policies
- Appendix 1: Personal data breach procedure

Policy Cover Note

Title of the Policy	Data Protection
Statutory Requirement Y/N	Y
Decisions to be made / recommendation on options	
Name of the author	
Date written	July 2026
Date for review	July 2028
Summary of amendments / updates to policy	Updated in July 2026 to reflect the latest ICO and DfE guidance for schools, academies and trusts, including the Data (Use and Access) Act 2025 changes now in force, the new statutory requirement to operate a data protection complaints procedure, updated DfE guidance on data protection in schools published on 17 June 2026, revised guidance on photos, videos, CCTV, generative AI, cyber security, filtering and monitoring, safeguarding data sharing, SAR handling and access to education records.

The Link Education Trust

Data Protection Policy

1. Aims

The Trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, 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 at each of our academies.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Privacy and Electronic Communications Regulations where relevant, and the Data (Use and Access) Act 2025. It is based on current guidance published by the Information Commissioner's Office (ICO), including guidance for schools, colleges and universities, UK GDPR guidance and resources, subject access requests, education information, data sharing, personal data breaches, CCTV and video surveillance, children's information and the Data (Use and Access) Act 2025.

It also reflects Department for Education guidance, including Data protection in schools, updated on 17 June 2026, and relevant statutory safeguarding guidance, including Keeping Children Safe in Education and Working Together to Safeguard Children, where personal data is processed or shared for safeguarding purposes.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • URN 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 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 accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data protection complaint	A complaint from an individual about how the Trust has handled their personal data or complied with data protection law. From 19 June 2026, organisations must have a clear process for receiving, acknowledging, investigating and responding to data protection complaints.

4. The data controller

The Trust process personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew or update this registration annually or as otherwise legally required. Where individual academies have separate controller responsibilities, the Trust will ensure that registration and privacy information accurately reflect those arrangements.

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 Trust Board

The Trust Board has overall responsibility for ensuring that each school 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 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 trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Our DPO is Cook Lawyers - Mr John Cook and is contactable via john@cooklawyers.co.uk

The DPO will also oversee the Trust's data protection complaints process, advise on data protection impact assessments, support lawful and secure data sharing, advise on the use of generative AI and education technology where personal data may be processed, and act as the Trust's contact point for the ICO and data subjects.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis at each school.

5.4 All staff

Staff are responsible for:

Collecting, storing and processing any personal data in accordance with this policy

Informing the school 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 our school 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 school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school 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 school, 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 school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers 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.

Where the Trust processes criminal offence data, including information connected with DBS checks, safeguarding concerns, allegations, investigations or related security measures, it will only do so where permitted by law, where an appropriate policy document or other required safeguards are in place, and where the processing is necessary and proportionate.

If we offer online services to pupils, including classroom apps, learning platforms, generative AI tools or other education technology, we will identify whether the supplier acts as a processor or controller, ensure that any processing is lawful, transparent and limited to what is necessary, carry out appropriate due diligence and data protection impact assessments where required, and obtain parental consent where consent is the lawful basis and the pupil is not able to provide valid consent themselves.

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

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted, securely destroyed, returned to the appropriate system or anonymised in accordance with the Trust's retention schedule and the DfE guidance on creating and maintaining a data retention schedule for schools.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carers 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
- 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

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

The Trust may share personal data without consent where this is necessary and proportionate for safeguarding purposes. It is not usually necessary to obtain consent before sharing information to keep a child safe, but staff must involve the designated safeguarding lead, share only what is necessary, use secure methods and record the decision, lawful basis and reasons for sharing.

Where we transfer personal data outside the UK, we will do so only where permitted by data protection law, including through adequacy regulations, the International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism, and after carrying out any required transfer risk assessment.

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 school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long will the data 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 can be made verbally or in writing, including by letter, email, online form, social media message or in person. Staff must not require a request to use particular wording or form before treating it as a SAR.

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 Headteacher and DPO.

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.

The Trust will consider each request involving a child on a case-by-case basis, taking into account the child's maturity, understanding, wishes and best interests. ICO guidance indicates that, where a child is under 12, a person with parental responsibility may generally be permitted to exercise the child's right of access, but this is not an automatic rule and staff must seek advice from the DPO where there is any doubt, dispute, safeguarding concern or risk of harm.

9.3 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
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

If the Trust refuses to comply with a SAR, or charges a reasonable fee, it will explain its reasons, advise the individual of their right to complain to the ICO and inform them of their right to seek a judicial remedy.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

The statutory time limit will usually begin when the Trust receives the request. If the Trust reasonably requires information to confirm the requester's identity, the time limit may pause until that information is received. The Trust will keep a clear record of dates, searches, exemptions considered, redactions and decisions made.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

The Trust will distinguish between a pupil's right of access under UK GDPR and any separate parental right to access a child's educational record under education regulations. In England, the separate parental right to access the educational record applies to maintained schools and special schools, including those not maintained by a local authority, but does not apply in the same way to academies, free schools or independent schools. Where the right applies, access must usually be provided within 15 school days of receipt of a written request. Where it does not apply, the Trust will consider the request under UK GDPR and seek DPO advice where required.

11. CCTV

We may use CCTV and other video surveillance in appropriate locations around the school site for specified purposes, such as security, safeguarding and the prevention or detection of crime. The Trust will follow ICO guidance on video surveillance and DfE guidance on taking and using photos and videos, and using CCTV in schools.

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 school office.

12. Photographs and videos

As part of day-to-day activities, the Trust may take photographs and record images of individuals.

The Trust will identify the purpose and lawful basis before taking or using photographs or videos of pupils, staff or visitors. Consent will usually be obtained for optional communication, marketing and promotional use, but may not be required for core educational, safeguarding, security or statutory purposes where another lawful basis applies. The Trust will clearly explain how images will be used to parents/carers, pupils and staff.

Uses may include:

- Within school on noticeboards, newsletters, etc.
- Outside of school by external agencies such as the school photographer, local newspapers
- Online - school website or social media pages (e.g. Twitter)
- Sale of DVDs from Christmas Performances

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

Before publishing images or recordings online, including on the school website, social media or learning platforms, staff must consider whether the image could identify a child, whether any safeguarding risks arise, whether the proposed use matches the information provided at the point of collection, and whether the child's best interests have been taken into account.

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

13. Data protection by design and default

The Trust 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 data protection impact assessments where processing is likely to result in a high risk to individuals' rights and freedoms, including when introducing new technologies, generative AI tools, biometric systems, extensive CCTV or monitoring, large-scale processing of special category data, or new data sharing arrangements. 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 the schools are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the Trust and DPO and all the information we are required to share about how we use and process their personal data (via The Trust privacy notices)
 - For all personal data that is held, 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 the trust is storing the data, retention periods and how we are keeping the data secure

- Maintaining a clear data protection complaints procedure which explains how individuals can complain, how complaints will be acknowledged, investigated and responded to, and how individuals can escalate unresolved complaints to the ICO.

14. 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 school office
- Strong passwords, multi-factor authentication where available, role-based access controls and secure account management are used to access school systems, laptops and other electronic devices. Default passwords must be changed, accounts must not be shared, and access must be removed promptly when no longer required.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- The Trust will maintain appropriate cyber security measures, including staff awareness, secure configuration, access controls, backups, malware protection, patching, incident reporting and secure filtering and monitoring arrangements where these involve personal data or safeguarding information.

15. 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 school/trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. 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, we will follow the procedure set out in appendix 1. If appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

The Trust will assess each incident promptly to decide whether it is a personal data breach, whether it is likely to result in a risk to individuals' rights and freedoms, whether it must be reported to the ICO within 72 hours of becoming aware of it, and whether affected individuals must be informed without undue delay because the risk is high.

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

17. Data protection complaints

Individuals may raise a data protection complaint if they are unhappy with how the Trust has handled their personal data, responded to an information rights request, shared information, used images or CCTV, handled a data breach, or otherwise complied with data protection law.

The Trust will provide a clear route for complaints to be made to the DPO or another nominated contact. The Trust will acknowledge a data protection complaint within 30 days of receipt, investigate it without undue delay, keep the complainant informed where appropriate, and tell them the outcome. Where a complaint is not resolved, the Trust will inform the complainant that they may complain to the ICO.

18. Training

All staff and trustees 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 school's processes make it necessary.

Training will include, as appropriate to role, recognising SARs and data protection complaints, secure data sharing, safeguarding information, use of generative AI and edtech, cyber security, phishing, data breach reporting, retention and deletion, CCTV/images, and the handling of special category and criminal offence data.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with Trust personnel and Trustees.

20. Links with other school policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online safety policy
- Acceptable use policy
- Safeguarding policy
- Data retention schedule
- Data breach procedure
- Data protection complaints procedure

- CCTV policy
- Image use and consent procedures
- AI and education technology acceptable use procedures

Delete where/if appropriate

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 Headteacher or nominated person
- 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 the school office
- 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 by the Trust and the DPO.

The DPO and the Trust will 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

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.

Sensitive information being disclosed via email (including safeguarding records)

- If a 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 we receive 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, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.