Data Protection Policy

Last reviewed: 7 April 2025

Contents

1. Aims

Discovery Summer aims to ensure that all personal data collected regarding staff, students, parents, English Student Hosts, Group Leaders, 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 digital format.

2. Legislation and guidance

This policy meets the requirements of GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. 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: • Health – physical or mental • Criminal record • Passport/ID • Safeguarding concerns
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.
Student	Throughout this policy any reference to 'students' also includes English Student Hosts
Host Centre	Organisations/schools from which we rent summer school premises

4. The data controller

Discovery Summer processes personal data relating to staff, job applicants, students, parents, group leaders, visitors and other individuals, and therefore is a data controller.

Discovery Summer 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 Discovery Summer, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Privacy Officer

The Privacy Officer is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The Privacy Officer is also the first point of contact for individuals whose data Discovery Summer processes.

Our Privacy Officer is Michael Johnson and is contactable via dpo@discoverysummer.com

5.2 Data Protection Compliance Manager

The Data Protection Compliance Manager – Jeremy Johnson - acts as the representative of the data controller on a day-to-day basis. He can be contacted via dpo@discoverysummer.com

5.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Discovery Summer of any changes to their personal data, such as a change of address
- Contacting the Data Protection Compliance Manager 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 we 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 fulfill 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 Discovery Summer 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 we can **fulfill a contract** with the individual, or the individual has asked us to take specific steps before entering into a contract
- The data needs to be processed so that we 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 we can perform a task **in the public interest,** and carry out our official functions
- The data needs to be processed for the **legitimate interests** of Discovery Summer or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent when appropriate in the case of a student) has freely given clear **consent**

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

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

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 or shredded. This will be done in accordance with Discovery Summer's data retention guidelines.

8. Sharing personal data

We will only share data with other organisations where:

- There is an issue with a student 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 students – for example, IT consultants, host centres. 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 students 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.

Please see the Privacy Notice for Students and their Parents/Guardians and the Privacy Notice for Staff and Job Applicants for further details.

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 Discovery Summer 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 by email to the Data Protection Compliance Manager, Jeremy Johnson, dpo@discoverysummer.com

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 Data Protection Compliance Manager.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents. For a parent 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 below the age of 13 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 of under- 13's will be granted without the express permission of the student. This is not a rule and a student'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, 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 student or another individual
- Would reveal that the student is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

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

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

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 we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to 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 digital format if necessary)

Individuals should submit any request to exercise these rights to the Data Protection Compliance Manager, Jeremy Johnson. If staff receive such a request, they must immediately forward it to the Data Protection Compliance Manager, dpo@discoverysummer.com

10. CCTV

All our host centres use CCTV cameras in various locations around the school/campus to ensure maximum security.

All host centres must adhere to the ICO's code of practice for the use of CCTV.

11. Photographs and videos

Discovery Summer is committed to ensuring the privacy of all its students and staff.

Photos/videos of students

As part of the Medical and Consent Form (which must be completed before the start of a student's course) their parents will be asked to opt-in to their child's photo being used for publicity purposes.

A student's full name never appears alongside their image.

If consent is given, photos/videos may be taken and used/shared in the following ways:

- Centre blog posts: our centre blogs are password-protected so that only those directly involved with the course (e.g. parents, staff, students, representatives) can view them
- On our websites and YouTube channels
- In our brochure and other printed publicity material
- Social media posts (currently Facebook, Instagram, Twitter, LinkedIn)
- With our representatives for their website/brochure
- With other professional organizations e.g. English UK, Quality English, TEN (The English Network)

We may continue to use these images/videos in future years.

If the parent does not consent for photos/videos to be used for publicity purposes we will only take/use the student's image in the following ways:

- The student's photo is taken on arrival and uploaded to our online database to help us identify and care for them
- Printed versions of group course/class photos are given to students at the end of the course
- In internal presentations
- With the police if the student goes missing

If students or their parents/guardians have any questions about how images are used, they should contact info@discoverysummer.com

Photos/videos of staff

When staff apply, they will be asked to opt-in to their photo being used for publicity purposes.

Please note that a staff member's full name will not appear alongside their image. If we would like to publish a staff member's full name alongside their image, we will ask for separate consent.

If staff member's give consent, photos/videos may be taken and used/shared in the following ways:

- Centre blog posts: our centre blogs are password-protected so that only those directly involved with the course (e.g. parents, staff, students, representatives) can view them
- On our websites and YouTube channels
- In our brochure and other printed publicity material
- Social media posts (currently Facebook, Instagram, Twitter, LinkedIn)
- With our representatives for their website/brochure
- With other professional organizations e.g. English UK, Quality English, TEN (The English Network)

We may continue to use these images/videos in future years.

If staff member does not consent for photos/videos to be used for publicity purposes we will only take/use their image in the following ways:

- On our staff database
- On notice boards around campus
- Printed versions of group course/class photos which are given to students at the end of the course
- In internal presentations
- With the police if the staff member goes missing

If staff have any questions about how images are used, they should contact info@discoverysummer.com

12. 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 suitable Privacy Officer and Data Protection Compliance Manager, and ensuring they have the necessary support
- 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 Discovery Summer's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- 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.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our company and Privacy Officer 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

13. 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 in a secure environment
- Papers containing confidential personal data must not be left on desks, pinned to notice/display boards, or left anywhere else where there is general access
- Device management software is installed on all Discovery Summer portable devices e.g. tablets, laptops, smart phones to ensure that data can be erased in the event of e.g. theft
- Staff who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Providing information over the phone

Any member of staff dealing with phone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity (following written guidance provided) to make sure that information is only given to a person who is entitled to it.
- In the case of a staff reference, request that the caller emails their request to the Discovery Summer Manager, Mary Shipley, mary@discoverysummer.com
- Refer to the Data Protection Compliance Manager for assistance in difficult situations. No-one should be bullied into disclosing personal 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.

e.g. Paper-based records will be shredded or incinerated and electronic files deleted. We may also use a third party to safely dispose of records on our 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

Discovery Summer will make all reasonable endeavors 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 may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a company laptop containing personal data about students
- The hacking of the Discovery Summer on-line database (portal)

17. Training

All staff 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 company's processes make it necessary.

18. Monitoring arrangements

This policy is regularly reviewed and will be updated as and when is necessary.

19. Links with other policies

This data protection policy is linked to our:

- Privacy notice for website visitors
- Privacy notice for students and their parents/guardians
- Privacy notice for staff and job applicants
- Safeguarding policy

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 Data Protection Compliance Manager
- The Data Protection Compliance Manager will investigate the report, and determine whether a breach has occurred. To decide, the Data Protection Compliance Manager 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 Data Protection Compliance Manager will alert the Managing Director
- The Data Protection Compliance Manager 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 Data Protection Compliance Manager will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Data Protection Compliance Manager 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 Data Protection Compliance Manager 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
    - 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 Data Protection Compliance Manager must notify the ICO.
- Where the ICO must be notified, the Data Protection Compliance Manager will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Data Protection Compliance Manager 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 Data Protection Compliance Manager
    - 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 Data Protection Compliance Manager 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 Data

Protection Compliance Manager expects to have further information. The Data Protection Compliance Manager will submit the remaining information as soon as possible

- The Data Protection Compliance Manager 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 Data Protection Compliance Manager 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 Data Protection Compliance Manager
    - 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 Data Protection Compliance Manager 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 Data Protection Compliance Manager will document each breach, irrespective of whether it is reported to the ICO in case it is challenged at a later date by the ICO or an individual affected by the breach.

  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 on the Discovery Summer Google Drive.
- The Privacy Officer, Data Protection Compliance Manager and Managing Director 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

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 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 Data Protection Compliance Manager as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the Data Protection Compliance Manager will recall it*
- *In any cases where the recall is unsuccessful, the Data Protection Compliance Manager 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 Data Protection Compliance Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The Data Protection Compliance Manager 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*