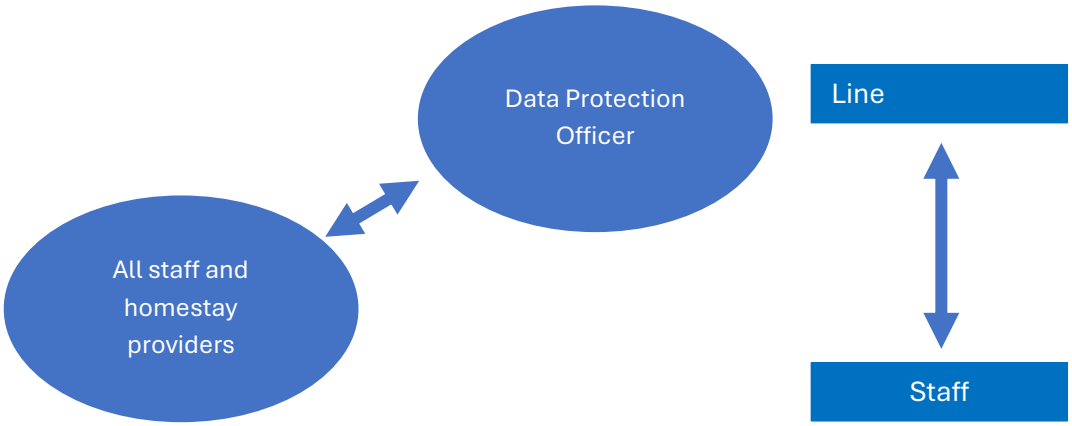
Privacy Policy and Procedures 2024

Date first issued	25 May 2018
Authored by	Dave Parsons In consultation with: Alex McDermott Dale McFarlane Ferdinando Eva Margaret Comber
Applies to	All staff
Reviewed	19 October 2024
Version	1/2024
Approved by	Chris McDermott, Principal
Linked to	*Privacy Notice Staff* *Privacy Notice Homestay Providers* *Privacy Notice Students and Group Leaders* *Staff Disciplinary Policy and Procedures 2024* *Parental Consent Forms* *Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO)* *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

Contents

Responsibility structure



Summary

The Privacy Policy and Procedures 2024 is a fundamental component of the School's administrative operation. It sets out the expected staff responsibilities and behaviours and customer outcomes for this important component of customer and supplier care.

Item	Summary	Responsible staff	References
Legal basis	Outlines GDPR principles	Data Protection Officer and data processors	Sections A and B
Students missing from excursions	Contact group leaders (to contact students directly). Liaise with management and/or emergency phone holder if/as necessary	Activity staff and management staff	B2

Statement

Broadstairs English Centre's *Privacy Policy and Procedures 2024* results from a commitment to the health and safety of all its stakeholders. The School wrote this procedure as a result of the implementation of the General Data Protection Regulation (GDPR) across the European Union, with effect from 25 May 2019. From January 1 2021 the UK GDPR came

into effect. The ICO website states "The 'UK GDPR' sits alongside an amended version of the DPA 2018". Effectively, the day-to-day procedures remain the same under UK GDPR.

Context

At Broadstairs English Centre we are committed to handling the personal data of all stakeholders in a safe, secure and transparent manner.

This policy sets out the principles and framework for a clear and consistent strategy for ensuring that all stakeholders' data is collected, stored and used in line with the requirements of the UK General Data Protection Regulation (GDPR) and that all stakeholders are made aware of what data is collected and how it is stored and used and how they may request access to any personal data that is collected.

Responsibility

Responsibility for ensuring that the *Privacy Policy and Procedures 2024* is implemented and known to all relevant parties is ultimately with the Data Protection Officer (DPO). However, it is the responsibility of all members of staff to ensure that the basic principles of secure data handling are adhered to at all times. The responsibility for drafting the policy and procedure and carrying out any associated risk assessment is with the Data Protection Officer (DPO) and the Director and the Director of Studies (as policy and procedure editor) and any consultants.

Definitions

Data Protection Officer (DPO) – ensures that an organization applies the laws protecting individuals' personal data
Data controller – the person (or business) who determines the purposes for which, and the way in which, personal data is processed
Data processor – anyone (other than an employee of the data controller) who processes personal data on behalf of the data controller

The key points of the policy statement are:

A: Principles

B: Data collection

A: Principles

A1: Core principles

Broadstairs English Centre's *Privacy Policy and Procedures 2024* governs any kind of process where the School is acting as a data controller of personally identifiable information. The policy applies to processing of data collected by any means. Any

questions regarding data processing should be directed to the School's Data Protection Officer at margaret.comber@broadstairsenglish.com.

A1.1: Data processing principles

The following principles are applied when processing personal data:

- personal data is only collected for specific and specified purposes; it is made clear when the information is requested (whether as part of a contract, or as a discrete consent-based request), why it is being collected and how it is to be used
- no unnecessary personal data is requested; we minimise the amount of information we collect to what we need to deliver the services required/offered
- personal data is only collected when there is a sensible business reasons for doing so
- personal data will only be used for reasons other than those stated at the time of collection with the consent of the data provider
- personal data will be up-dated periodically; we accept requests for amendments to personal data from data providers; all data providers have the right to request what personal data is being held and to be made aware of how it is being stored, used and (if applicable) shared with others
- personal data is kept secure by following the guidelines of our IT partner, Cyber Central Limited, Broadstairs (in the case of electronic storage and transmission) and by following the procedures governing the safe collection, storage and use of hard copy (paper-based) information included in the procedures section of this document
- personal data will not be stored for longer than is necessary to accomplish its purpose, or as is required by law

B: Data collection

B1: When personal information is collected

Personal information (data) is collected in several situations, which fall broadly into four categories:

- when someone applies to join a course at the School (either as a member of a school (educational) group or through an Education Travel Organisation (agent/agency)
- when someone applies to join the School as a member of staff
- when someone applies to become a homestay provider for the School
- in some circumstances where someone interacts with the School website or requests information or services that require the collection of some personal data for that information or service(s) to be provided

B1.1: Personal information collected when someone applies to join a course at the School

When someone applies to join a course at the School (either as a student, or in the capacity of a group leader) we collect, store and process the following personal data:

- full name

- address (may be collected discretely or as part of the *Parental Consent Forms* for students who are members of groups and under the age of 18 or vulnerable adults)
- contact telephone numbers (as above)
- date of birth
- gender (required for compliance with British Council criterion W7 – privacy from members of the opposite sex)
- nationality (required for compliance with British Council criterion W15 – students with the same first language…)
- first language (see above)
- passport number (if required for visa applications)
- photo (if required)
- next of kin contact details
- course and language capability details (if required)
- medical details, including allergies and food intolerances, disabilities and special educational needs
- police check information to ensure that those adults who are accompanying students under the age of 18 (and/or vulnerable adults) are fit and proper persons to do so

B1.2: Personal information collected when someone applies to join the School as a member of staff

When someone applies to join the School as a member of staff (either full- or part-time, temporary or permanent contract) we collect, store and process the following personal data:

- full name
- address
- contact telephone numbers
- contact email address
- date of birth
- curriculum vitae and professional references
- proof of ID
- Enhanced DBS certificate
- proof of qualifications (where applicable)
- employment contract
- bank details (for wage/salary payments)
- national insurance number (for wage/salary payments)
- medical details, including allergies and food intolerances, disabilities and special educational needs
- nationality (to ensure right to work in the UK etc.)

B1.3: Personal information collected when someone applies to become a homestay provider for the School

When someone applies to become a homestay provider for the School we collect, store and process the following personal data for the primary (named) provider:

- full name
- address
- contact telephone numbers
- contact email address
- date of birth
- bank details
- personal references
- risk assessments on the homestay provider's property
- gas safety certification
- driving licence, car insurance and MOT (for driving homestay providers)
- ages of all residents
- criminal records check to establish suitability to be in contact with children under the age of 18 (DBS certificate)
- feedback from customers on their homestay experience

We also collect the following personal data for any other adults in the household (over and above the primary (named) homestay provider):

- full name
- date of birth
- occupation

B1.4: Personal information collected in some circumstances where someone interacts with the School website or requests information or services that require the collection of some personal data for that information or service(s) to be provided

When someone interacts with the School website or requests information that require the collection of some personal data, such data collection will be limited to that which is the minimum required to carry out the request for information or services being made. Typically, this is will be:

- name
- contact number
- any other relevant information

In all cases respondents will be told why the information is required and whether it is to be stored, used or shared. In these cases, the legal basis for the data collection is consent based on the fact that the request is initiated by the enquirer. The legal bases may also be contract or legitimate interest, depending on the nature of the enquiry.

B2: Access to personal data

Who has access to the personal data of customers (students and group leaders), staff and/or homestay providers (and other contracted suppliers etc.) varies from category to category depending on need.

B2.1: Who has access to the personal data of customers (students and group leaders)

The following people have access to some, or all, of the personal data of students and group leaders for various operational reasons:

- the Director
- members of the accommodation department
- members of the activities department
- Education Travel Organisations (agents)
- the Bookings and Enrolment Manager
- the Accounts Managers
- front of house staff and member of staff holding the emergency phone
- catering providers

B2.2: Who has access to the personal data of staff

The following people have access to some, or all, of the personal data of staff for various operational reasons:

- the Director
- the employee's line manager
- the Accounts Manager

B2.3: Who has access to the personal data of homestay providers

The following people have access to some, or all, of the personal data of homestay providers for various operational reasons:

- the Director
- members of the accommodation department
- the Accounts Manager
- front of house staff and member of staff holding the emergency phone
- members of the activities department
- Education Travel Organisations (agents and schools)
- the Bookings and Enrolment Manager

B2.4: Who has access to the personal data collected via the website or through personal enquiries

The following people have access to some, or all, of the personal data collected via the website or through personal enquiries for various operational reasons:

- the Director
- the Accounts Manager
- front of house staff and member of staff holding the emergency phone

- the Bookings and Enrolment Manager

B3: Sharing of personal data

In order to fulfil our regulatory and contractual obligations we need to share personal data with third parties on occasion. Similarly, we need to share some personal data with outsourced suppliers that we have chosen to engage to meet our operational requirements. In all cases we limit the personal data that we share to only that which is necessary for them to perform the function/role that they have been contracted to perform. We will never sell personal data to any third parties. We take every precaution to keep personal data secure and to ensure that any third parties also have a robust policy and procedures in place to maintain the level of data security.

Personal data of students and group leaders may be shared with:

- Education Travel Organisations (agents)
- Inspectorates, regulatory bodies and other contracted service providers, e.g. British Council, IT support contractors
- homestay providers
- government agencies, e.g. the Home Office
- taxi and airport transfer providers
- other schools or venues that need information to ensure student and group leader health and safety, e.g. on immersion courses with shared classes in UK state schools

Personal data of staff may be shared with:

- Inspectorates, regulatory bodies and other contracted service providers, e.g. British Council, IT support contracts
- government agencies, e.g. the Home Office, DBS

Personal data of homestay providers may be shared with:

- Inspectorates, regulatory bodies and other contracted service providers, e.g. British Council, IT support contracts
- government agencies, e.g. the Home Office, DBS

B4: Retention of data

Personal data is retained for the duration of the contract under which it was collected (as a booking, an employment contract or a homestay provider contract, etc.) and then for a further five years to enable us to meet our regulatory and legal obligations. A secondary reason for retaining personal data of customers (students and group leaders) is for ease of administration for returning customers, to ensure that course content is not repeated, for example. An additional reason for retaining personal data or customers and homestay providers is to update interested parties as to what may be happening of interest to them at the school.

After five years all electronic records will be deleted, and any paper records destroyed (shredded).

B5: Legal bases for processing data

The General Data Protection Regulation (GDPR) establishes six legal bases for processing personal data:

- consent
- contract
- legal obligation
- vital interests
- public task
- legitimate interests

See the Information Commissioner's Office (ICO) website for definitions of these bases.

At Broadstairs English Centre we use different legal bases for collecting personal data depending on the purpose of the collection:

- contract is the legal basis for personal data collection used for:
    - making bookings to attend courses at the School
    - following recruitment and selection policies and procedures and employment offers at the School
    - following policies and procedures for contracting homestay providers
- legitimate interest is also a legal basis for personal data collection that may be applied to the situations (or some parts of them) outlined in the above bullet point
- legal obligation is also a legal basis for personal data collection that may be applied to the situations (or some parts of them) outlined in the above bullet points

B6: Special category data and criminal record data and parental consent forms

The School requests health data from potential students, group leaders and employees. This data has special protection under the GDPR (under Article 9(2)), that processing is necessary to protect the vital interests of the data subject (or another natural person where the data subject is physically or legally incapable of giving consent), or where processing is necessary for the purposes of preventive or occupational medicine or the assessment of the working capacity of an employee.

The School has safeguarding responsibilities and carries out DBS checks on all staff and other people who are likely to have direct supervisory responsibility for or unsupervised contact with people under the age of 18 (or vulnerable adults).

Parental Consent Forms are used to gain consent from parents for the provision of the School's courses and services for students under the age of 18.

B7: Managing concerns about personal data collection

All persons who have data collected about them (data subjects) have the right to request to see what information is held about them. It is important that data is correct and current. To ensure this the School will annually audit the information held and ask data subjects to update their information as appropriate.

If a data subject is aware of any inaccuracies in the data, it is their responsibility to contact the School to remedy any such inaccuracies. Contact margaret.comber@broadstairsenglish.com.

If a data subject wishes to request to see the data the School holds on them, provision of this data will be subject to the payment of a fee (currently £10) and the supply of appropriate evidence of identity. We may withhold personal information that data subjects request to the extent permitted by the law.

If a data subject has a complaint regarding the handling of their personal data, they should contact margaret.comber@broadstairsenglish.com. In the unlikely event that any complaint cannot be addressed, data subjects should call the Information Commissioner's Office helpline on 0303 123 1113 (checked 19/10/2024).

B8: Changes to Broadstairs English Centre's Privacy Policy

Any changes made to this policy will be posted on the School website and hard copy versions printed to replace older versions. Data subjects are encouraged to periodically check for updates or changes to the Privacy Policy.

Privacy Procedures 2024

Broadstairs English Centre's *Privacy Procedures 2024* results from a commitment to the health and safety of all its stakeholders.

The key points of the procedure are:

A: Receiving and processing personal data

B: Utilising personal data

C: Storing and deleting personal data

A: Receiving and processing personal data

A1: From customers

Personal data is received from customers as part of the booking process. The legal bases for requiring customers to provide personal data are:

- contract
- legitimate interest
- legal obligation

These bases are applied to ensure that it is possible to safeguard the health and safety of customers and to enable the smooth running of the business operations. The personal data is collected mainly through the instrument of the parental consent form

(for those under the age of eighteen) and through booking forms for group leaders and adults.

A2: From employees and homestay providers

Personal data is received from employees as part of the recruitment and selection process. The legal bases for requiring employees to provide personal data are the same as those for customers outlined above in A1. Personal data is collected through CVs, references, certification and Disclosure and Barring Service checks. Bank details and other data required to process salaries are collected using standard government issue forms.

Personal data is received from homestay providers as part of the application process. The legal bases for requiring homestay providers to provide personal data are the same as those for customers outlined above in A1. Personal data is collected through an application form, references, certification and Disclosure and Barring Service checks. Bank details and other data required to process payments are collected using the in-house application forms.

A3: Processing personal data

Personal data is processed at BEC by:

- the Bookings Manager and the Enrolment Officer (for customers – students and group leaders)
- line managers in their recruitment and selection processes
- the Accommodation Department in the processing of homestay provider applications
- the Accounts Department in the processing of payments to employees and homestay providers

All data processors must ensure that they collect data only for the purposes stated when requesting the data and that the data is processed in the correct manner.

A3.1 Processing data of customers (students and group leaders)

Event/Step	Procedure	Responsible party
Enrolment form completed	The appropriate enrolment form is completed by agents, group leaders or students. (Forms include a GDPR notice.) Forms are submitted to the Enrolment Officer (or the Bookings Manager for forwarding to the Enrolment Officer).	Agent(s) Group leader(s) Student(s) (or their parent(s)/ guardian(s))

Data processing	Completed enrolment forms are collected by the Enrolment Officer and data is imported into the School database.	Enrolment Officer
Parental consent form completed	All students under the age of 18 must provide parental consent from their parent(s) and/or guardian(s) for their stay at the School. Data is collected primarily from on-line parental consent forms. (Occasionally paper forms are used as a substitute.) Data from on-line forms is imported to the School database by the Enrolment Officer. (Information from paper forms is manually inputted by the Enrolment Officer.)	Enrolment Officer

A3.2 Processing data of employees (recruitment and selection)

Event/Step	Procedure	Responsible party
Recruitment and selection	As part of the recruitment and selection process applicants provide personal data to the School. Initially this is provided to whoever is the lead manager in the recruitment process. Applicants are informed of the reasons for data collection, the School policy regarding GDPR and their rights regarding the use of and their own access to the data.	Lead manager(s) in the recruitment process
Data processing	Personal data of successful applicants required for recruitment purposes and for payroll is given to the HR Manager who keeps both paper and electronic HR and payroll records. Copies of any relevant certificates or other documents are given to the HR Manager.	HR Manager

A3.3 Processing data of homestay providers

Event/Step	Procedure	Responsible party
Application	As part of the application process potential homestay providers provide personal data to the School. Initially this is provided to whoever is the Accommodation Department via an application form (which includes a GDPR notice).	Accommodation Department
Data processing	Personal data of successful applicants required for student placement is entered on to the School	Accommodation Department

	database. Personal data required for payroll is passed to the HR/Accounts Manager(s). Copies of any relevant certificates or other documents are given kept by the Accommodation Department. Original application forms are filed (see section on storage of data below).	HR Manager/ Accounts Manager(s)

B: Utilizing personal data

Personal data, once collected, is used by the School for the following purposes:

- Student administration
- Employee administration

B1: Student administration

Personal data is used in student administration to ensure the health and safety of students during their stay at the School.

B1.1: Teaching department documents

Lesson registers, class lists, alphabetical lists and other student administration documents do not contain personal information that is likely to cause an issue under UK GDPR regulations. Student administration documents do not contain any more information than (at most) name, age and gender. Teaching documents that contain personal data are not generally customer facing.

Event/Step	Procedure	Responsible party
Generating teaching documentation	Registers, class lists, alphabetical lists, end of course questionnaires, certificates, course reports, test results, are all generated from the School database by using buttons that run the necessary queries.	Teaching Department Administrative Assistant(s)
Use of documents	Teachers should keep all documentation secure. Daily registers should be returned to the DOS office at the end of each morning and/or afternoon teaching session. End of course questionnaires should be returned to the DOS office on completion. Any other paperwork that has any personal data within it should be shredded at the earliest opportunity.	Teaching staff

B1.2: Activity department documents

Activity registers contain student name, age and gender and homestay provider names (anonymised), addresses and telephone numbers. Registers are headed with the wording “to be shredded at the end of the activity”. Activity department registers are not generally customer facing.

Event/Step	Procedure	Responsible party
Generating activity registers	Activity registers are generated from the School database by using a button that runs the necessary query.	Activity Department
Use of documents	Activity staff should keep all documentation secure. Daily registers should be shredded at the earliest opportunity after each activity.	Activity Leaders

B1.3: Accommodation department documents

Activity Department documents include group registers, homestay provider allocations, student ID cards. These documents contain some or all the following, homestay provider names (anonymised), addresses and phone numbers. Accommodation department documents are not generally customer facing, they are shared with agents, group leaders and individual homestay providers. Student ID cards are given to individual students.

Event/Step	Procedure	Responsible party
Generating accommodation department documents	Accommodation Department documents are generated from the School database by using buttons that runs the necessary queries.	Accommodation Department Administrative Assistant(s)
Use of documents	Accommodation Department staff should keep all documentation secure. Unneeded documents should be shredded at the earliest opportunity.	Accommodation Department staff

C: Storing and deleting data and subject access requests (SARs)

The storage and deletion of data is central to GDPR. Any information held must be held securely and only shared with others within and outside the organisation as required by operational procedures. Storage of hard copies is in lockable filing cabinets (that are always locked when not in use). Electronic storage is managed by limiting access to

data from unauthorized users by means of password protection and/or secured folders on the network.

Persons whose data is held by the School may request access to the information held about them. These are known as Subject Access Requests. The School must allow access to the data but can charge an administration fee for the facilitation of the request. For 2024 the administration fee is set at £20 per request, to be applied at the School's discretion. The School will usually be expected to fulfil the SAR within one month. The SAR may request ALL data that is held referring to the subject. The School may refuse some parts of a request but must have a justifiable reason for doing so. Where information held relates to other parties as well as the subject, redaction is likely to be required. For more information for organizations and individuals visit https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/

C1: Storing data

Event/Step	Procedure	Responsible party
Hard copies	All hard copies of documents that include personal data to be stored in lockable filing cabinets (that are always locked when not in use). Offices to be locked out of office hours.	All staff with access to lockable filing cabinets and/or offices
Electronic data	All electronic documents that include personal data to be stored on computers that either require password access to utilise the computer and/or require authorisation from system administrators to view folders that contain such information.	All staff with access to lockable filing cabinets and/or offices

C2: Deleting data

Event/Step	Procedure	Responsible party
Hard copies – operational documents	All hard copies of documents that include personal data that have been issued for operational purposes and are no longer needed should be shredded at the earliest opportunity, e.g. registers, hosting lists, etc. (other than reference copies that are kept securely in the relevant departmental offices).	DPO Data controllers

Hard copies – stored data	All hard copies of documents that contain stored personal data, e.g. recruitment and selection/HR information, homestay provider information, etc. are kept for five years after the end of the employment/ retention of the person(s) involved. At the end of this period information is deleted.	DPO Data controllers
Electronic data	Electronically-stored personal data are kept for five years after the end of the employment/retention of the person(s) involved. At the end of this period information is deleted. Electronically-stored personal data of customers is deleted one-week after their departure (except in circumstances where an on-going investigation of some kind may require an extension of this period).	DPO Data controllers

D: DPO – Data Protection Impact Assessment (DPIA)

The School has an appointed Data Protection Officer (DPO) and is certified with the Information Commissioner's Office (ref. number ZB415270). Current registration expires on 19/10/2025 and will then be renewed (two years at a time). As part of the certification process the DPO carries out a Data Protection Impact Assessment (DPIA) which risk assesses the handling of personal data within the organisation.

E: Day-to-day good practice

All employees should follow the rules of UK GDPR and be made aware of the principles and the reasoning behind them.

Employees should be encouraged to ensure that:

- No personal data is left in situations where it may be viewed by others. This includes keeping phone numbers, email addresses, etc. in lists on walls in offices – for example; leaving registers etc. on reception counters, etc.
- Hard copies of information are shredded once they have served their immediate purpose
- The habit of "clean desks" is followed – no information should be left out overnight on desks, for example
- Computer screens are locked when unattended (Windows key and L)

F: Data breaches

A data breach occurs when an individual's personal data is shared with others who are not listed as having authority to access that data.

The most common data breach is likely to be sharing email addresses of individuals by failing to use the BCC facility in multiple-addressee emails. Any such breaches should be noted and all affected parties should be informed that the breach has happened. Staff should be reminded of the need to use BCC as a default when emailing multiple recipients outside the organisation.

There may be other internal instances of data breaches. These may be employees being negligent in handling data (most often in hard copy) or, in a worst-case scenario, acting illegally with intention. In each case, the School will act on a case-by-case basis to ensure that the appropriate action is taken and that all affected parties are informed of all remedial actions taken.

External factors are likely to be malicious/criminal in intent and could be hacking, phishing or other data mining activities. The School will protect itself from these events by ensuring that all stakeholders are aware of good digital practices. These include:

- Not opening emails from unknown recipients without first checking whether the email address(es) appear to be legitimate
- Ensuring that emails from "known" recipients actually originate from legitimate email addresses. It is particularly common for "invoices" to be used as a means of accessing systems
- Firewalls and other filters are up-to-date and fit for purpose

Note

This policy and procedure was reviewed and updated on 19 October 2024. Reference to SARs has been included. Section E, Day-to-day good practice has been included. Section F, Data breaches has been included.