Ballymun Educational Support Team CLG

Data Protection Policy

Document Reference No.	Policy XX	Document Developed by	Hazel Walsh/Marian Barnard
Version Number	V2	Document Approved by	BEST Board
Approval Date	October 2021	Responsibility for Implementation	All Staff
Revision Due Date	October 2023	Responsibility for Review and Audit	DP Officer

Contents

1.0 Policy Statement

All those who provide Ballymun Educational Support Team CLG ("BEST") with their Personal Data have a right to respect and privacy in relation to their data. In addition, the statutory obligations under the Data Protection Acts 1988 & 2003 together with the General Data Protection Regulation that came into force on 25th May 2018 (the GDPR) must be strictly adhered to.

This Policy Statement is written to address these moral and legal obligations. BEST collates, processes and controls Personal Data in respect of our Students, Parents, Teachers, Volunteers, Employees and Service Providers and in accordance with GDPR BEST is a Data Controller. BEST acknowledges its responsibility for ensuring the privacy of data subjects and for the protection of their personal data within BEST. It is the policy of BEST to meet these obligations to the highest standards possible.

This policy sets out how BEST protects personal data and sets out the rules governing the use of personal data provided to BEST. Appendix 1 outlines the definition of terms in relation to the Data Protection Standards.

2.0 What is Personal Data?

Personal Data is any personal information that relates to a living individual. The law sets out a series of standards which any person or entity must adhere to when collecting, storing or using such data. This law applies regardless of:

- how trivial or non-intrusive it may be, or
- whether it is collected directly from the person in question or from another source.

3.0 Types of Personal Data held in BEST

BEST recognises the need to hold personal data about individuals for the following purposes:

- Information relating to service provision across our services and programmes in relation to Students, Parents and Teachers
- Information on volunteers
- Data base and mailing information
- Event Management
- Information on stakeholders in relation to fund-raising and service development
- Information relating to research
- Human Resources information relating to recruitment and staff management

At each point of data collection, it is imperative to be clear to individuals about the purposes for which that information is being or will be, utilised for and only use it for these purposes unless permission is given for additional uses.

BEST collects and uses Personal Data as follows:

a) In respect of Students and Parents:
   - Name, address, telephone, email & other contact details
   - Signatures
   - Date of birth
   - Nationality
   - Interactions with BEST staff on the premises, by phone or email
   - Current or past complaints

b) In respect of Employees:
   - Name, address, telephone, email & other contact details.
   - Identification documents
   - Date of birth, career history, educational background, details of certificates and diplomas, skills, job title, CVs, bank account details, nationality & other information collected for employment purposes (not Volunteers)
   - PPSNs
   - Sickness Certificates and other required health information
   - Next of Kin

c) In respect of Volunteers (Board Members):
   - Name, address, telephone, email & other contact details.
   - Identification documents
   - Date of birth, career history, educational background, details of certificates and diplomas, skills, job title, CVs, bank account details, nationality & other information collected for employment purposes (not Volunteers)
   - PPSNs

d) In respect of Suppliers and Service Providers:
   - Name, address, telephone, email & other contact details.
   - Identification documents
   - Bank Details

The data that BEST collects can be sensitive in nature and is collected, processed and stored in line with GDPR:

- Client's names are not used on electronic mail, both internally and externally
- All client files are anonymised using client codes and stored on a secure server. These codes are also used when collating statistics or reporting
- If it is necessary to keep a physical file, these are held in locked filing cabinets at BEST's offices

The types of data BEST collects and how it is stored is highlighted in Appendix 18.

BEST also has a Confidentiality Policy and uses Consent Forms for parents and students / young people where necessary, which form an integral part of ensuring that BEST adheres to the Data Protection Acts 1988 & 2003 and the General Data Protection Regulation 2018.

The information that is collected is necessary to allow BEST to carry out its day-to -day operations, to meet its objectives and to comply with legal and regulatory obligations including but may not be limited to the following:

- School Completion Programme services in schools in our catchment area in Ballymun these include;
  - St Josephs Junior NS
  - St Josephs Senior NS,
  - Virgin Mary Boys NS,
  - Virgin Mary Girls NS,
  - Holy Spirit Girls NS,
  - Holy Spirit Boys NS,
  - Scoil an tSeachtar Laoch and
  - Trinity Comprehensive Secondary School.
- compliance with our legal, regulatory and corporate governance obligations and good practice
- ensuring business policies are adhered to (such as policies covering email and internet use)
- operational reasons, such as training and quality control, ensuring the confidentiality of sensitive information
- investigating complaints
- checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- monitoring staff conduct, disciplinary matters
- marketing BEST
- any other service(s) offered by BEST

In particular, this policy requires BEST staff to ensure that the Data Protection Officer (DPO) should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. BEST is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulation (GDPR) and national data protection legislation.

4.0 The legal obligations

Article 5 of the General Data Protection Regulation (GDPR) sets out key principles which lie at the heart of the general data protection regime. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation. Therefore, compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR. The following is a brief overview of the Principles of Data Protection found in article 5 GDPR:

Principle 1 Lawfulness, fairness, and transparency: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

Principle 2 Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and

legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

Principle 3 Data Minimisation: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

Principle 4 Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

Principle 5 Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. To ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Principle 6 Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 7 Accountability: Finally, the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with GDPR and be able to demonstrate (through appropriate records and measures) their compliance, in particular to the DPC.

In addition, the following requirements are included in the legislation:

a) A requirement for some Data Controllers to register with the Data Protection Commissioner – this is not necessary for BEST as it is a registered not-for-profit organisation

b) A requirement to safeguard Personal Data if its processing is outsourced to a third party

c) A prohibition of transferring Personal Data outside the European Economic Area unless in accordance with the Act.

BEST collects Client Data under Principle 2: Personal Data must be kept only for specified, explicit and legitimate purpose(s). In addition to the above, BEST prohibits any Employees from disclosing (or permitting to be disclosed) any information that concerns a Client with any other part of BEST's services, where it is necessary in order to support that Client fully.

Appendices 2 to 8 explain how BEST meets its obligations under each of the Data Protection Principles as well as additional requirements under the Data Protection Act. Appendices 9 to 19 illustrate BEST's procedures and documents to comply with GDPR requirements.

5.0 Data Register

One of the primary changes introduced by the GDPR is the requirement to have a comprehensive Data Register which contains the following elements:

- Categories of Personal Data and Data Subjects
- Elements of Personal Data included within each data category
- Source of the personal data
- Purposes for which personal data is processed
- Legal basis for each processing purpose
- Special categories of personal data
- Legal basis for processing special categories of personal data
- Retention period

BEST Data Register is shown in Table 1.

Table 1 BEST's Data Register

Data Set / Data Subjects	Source of Data/Purpose of processing/legal basis/Category of Data	Retention/Final disposition
Governance documents **Board, Volunteers and Staff**	Governance documents To satisfy Governance requirements Legitimate Interest Confidential	To be held Permanently.
Client Documentation		
Students and young people engaged with BEST SCP services	Notes and profile details Anonymous and kept separate from the electronic, primary or secondary file. Legitimate Interest / Consent Special Category Information (sensitive)	Paper files destroyed after **seven years** by shredding. Electronic Files deleted after seven years.
Parents of students and young people	Individual records of the persons accessing BEST services Paper and electronic records Legitimate Interest / Consent	Retained for **seven years** after the most recent discharge date.
Teachers and Schools	Individual records of the persons accessing BEST services Paper and electronic records Legitimate Interest / Consent	Retained for **seven years** after the most recent discharge date.
Child Protection Reports **Adult Service Users and their children**	Child Protection Reports Electronic Reports Legal basis Special Category Information (sensitive)	To be held Permanently.

Client Information for statistical / Audit purposes	Paper and electronic records Information to be held anonymously Legitimate Interest Confidential	There will be **no time limit** on such information being retained as this will be anonymous.
CCTV in BEST Offices (not currently used)	Electronic record Security Reasons Legitimate Interest Confidential	28 days
Administration		
Outsourced Service Provider Documentation	Contracts, bank details, correspondence etc. Service Provision Contract Confidential	Permanently as data protection obligations extend beyond the contract.
Financial Accounts	Bank details, ppsns, financial information Service Provision Legitimate Interest Highly Confidential	Statutory records – permanently Revenue filings – 6 years General documentation – 6 years
Complaint Handling	Complaints Governance Requirement Legitimate Interest Highly Confidential	6 years from date of final communication regarding complaint.

Human Resource Documentation		
Health Information and sick leave records	Sick Certs, Health information HR Legislation and Policy Contract Health information - Sensitive	A minimum of 3 months but potentially up to 6 years after employment ends - destroy by confidential shredding or electronic deletion
Time sheets	Timesheets HR Legislation and Policy Contract Confidential	2 years - destroy by confidential shredding or electronic deletion
Records of staff training	Training Records HR Legislation and Policy / Training Policy Legitimate Interest Confidential	5 years - destroy by confidential shredding or electronic deletion
Job description	Job Description HR Legislation and Policy Contract Confidential	Retain indefinitely and Archive
Applications and CV's of candidates who are called for interview	Applications HR Legislation and Policy Contract Confidential	Retain for 6-12 months after closing of competition and destroy by confidential shredding or electronic deletion

Selection criteria	Applications HR Legislation and Policy Contract Confidential	Retain indefinitely and Archive
Candidates not qualified or short listed	Applications HR Legislation and Policy Contract Confidential	Retain list of candidates who applied but destroy material such as application forms & CVs after 6-12 mths by confidential shredding or electronic deletion.
Candidates short listed but not successful at interview or who are successful but do not accept offer	Applications HR Legislation and Policy Contract Confidential	6-12 months - destroy by confidential shredding or electronic deletion
Interview marking sheet and interview notes	Marking Sheets HR Legislation and Policy Contract Confidential	6-12 months - destroy by confidential shredding or electronic deletion
Finance / pension / retirement records	Pension Policies HR Legislation and Policy Legitimate Interest Highly Confidential	Retain until pensioner and dependent spouse are deceased and destroy by confidential shredding or electronic deletion
Staff Personnel Files	HR Files HR Legislation and Policy Legitimate Interest	Retain for duration of employment. On retirement/resignation hold for further six yrs,

	Highly Confidential	retain service records for finance/pension purposes.
Application CV Referees	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	See above
Recruitment medical	HR Files HR Legislation and Policy Legitimate Interest Special category of Data (Sensitive)	See above
Contract/Job specification/ Job description	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	See above
Probation forms	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	See above
Parental leave	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	7 years - destroy by confidential shredding or electronic deletion
Discipline records	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Hold on personal file/disciplinary file for duration of employment plus six years after resignation/retirement, then destroy. Where

		disciplinary policy provides for earlier removal destroy but keep a record that a warning was issued. Where the matter involved criminal activity, these records should be retained indefinitely. Destroy by confidential shredding or electronic deletion
Allegations and complaints	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Where the complaint is found to be untrue or unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future.
Occupational health records	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Depending on the types of materials to which the staff member was exposed (e.g. carcinogens) the health screening reports may need to be retained for up to 40 years. Consult with your local Health & Safety Officer about retention periods for this class of record.
Industrial relations files	HR Files HR Legislation and Policy Legitimate Interest	Hold policy documents and the history of their evolution indefinitely. Archive

	Highly Confidential	
Agreements-pay and others	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Retain indefinitely and Archive
Minutes of meetings	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Retain indefinitely and Archive
Labour Court Recommendations	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Retain indefinitely and Archive
Contracts for services Examples of contracts for services that may be held by Personnel/HR departments include EAP contracts with service providers and contracts with healthcare professionals.	HR Files HR Legislation and Policy Legitimate Interest Highly Confidential	Retain for the duration of the contract plus six years and destroy by confidential shredding or electronic deletion

Note: Data is held in a mixture of electronic and paper data. Where possible electronic data is used but where this is not possible or for historic information paper files are in place.

Appendices 15 to 17 provide details of archiving and destruction of records.

6.0 Data Breach Reporting

The GDPR defines a Personal Data breach as meaning "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

BEST employees are required to notify the DPO where they identify or suspect that a data breach has occurred.

In accordance with GDPR, the DPO will notify the Data Protection Commission without undue delay where a breach is likely to result in a risk to the rights and freedoms of the Data Subject(s) involved.

The DPO will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the DPO will arrange for the data subjects to be notified.

If a BEST Employee knows or suspects that a personal data breach has occurred, they must not attempt to investigate the matter. They must immediately consult the DPO who will instigate an initial investigation, notify the Manager and the Data Protection Regulator if a data breach is suspected. All evidence relating to the potential personal data breach must be preserved.

7.0 Data Subject's Rights and Requests

The data subject has rights when it comes to the handling of their personal data, and they may:

- Withdraw processing based on consent at any time
- Receive certain information about the Data Controller's processing activities
- Request access to their personal data that we hold (-see Appendix 13)
- Prevent the use of the personal data for direct marketing purposes
- Request BEST to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Restrict processing in specific circumstances
- Challenge processing which has been justified on the basis of legitimate interests or in the public interest
- Object to decisions based solely on automated processing, including profiling
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

BEST will verify the identity of an individual requesting data under any of the rights listed above. (They should never allow third parties to persuade them into disclosing personal data without proper authorisation).

BEST Employees must immediately forward any data subject request received to the DPO and comply with the data access request procedure.

8.0 Data Protection Training

All BEST Employees receive training in respect of data protection. New joiners will receive internal training as part of their induction process, as per BEST's Induction Checklist. Further training will be provided at least annually or whenever there is a substantial change in the law or BEST's policy and procedures. Training is provided via attendance at internal/external training courses and induction for new starters.

The manager will continually monitor training needs but if BEST Employees feel that further training on any aspect of the relevant law or our data protection policy or procedures is required, they may contact the DPO directly.

9.0 Data Protection Impact Assessment

BEST Employees must conduct a **Data Protection Impact Assessment** (and discuss any findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

i. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes)

ii. automated processing including profiling and automated decision making

iii. large scale processing of Special Category Data (such as health)

iv. large scale, systematic monitoring of a publicly accessible area

A DPIA will include:

a) a description of the processing, its purposes and BEST's legitimate interests if appropriate

b) an assessment of the necessity and proportionality of the processing in relation to its purpose; an assessment of the risk to individuals

c) the risk mitigation measures in place and demonstration of compliance

10.0 Direct Marketing

BEST is subject to certain rules and privacy laws when marketing. BEST has identified consent as the legal basis upon which it will conduct direct marketing.

A data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing clients known as "soft opt in" allows marketing texts or emails to be sent if contact details have already been collected in the course of providing services to that person however the data subject must have, been given an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing is explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a person opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

11.0 Sharing Personal Data

Generally, sharing personal data with third parties is prohibited under law unless certain safeguards and contractual arrangements have been put in place.

BEST Employees may only share the personal data held by BEST with another employee, officer, agent or representative of BEST (if the recipient has a job/position-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions).

BEST will only share the Personal Data with third parties, such as service providers if:

i. Individuals are made aware of all requests for disclosures to third parties, and consent is always sought in advance for such disclosures.

ii. Disclosures are typically related to the further provision of service to an individual and consent for this is explicitly sought using the BEST Consent Form.

iii. Information disclosed to third parties may be in written or verbal form. All requests for information by individuals for information held on them by BEST.

iv. If disclosure of personal data to a third party is required which exceeds the terms of the provision within the consent declaration on the BEST consent application form, additional consent will always be sought in such cases.

v. Letters to external agencies containing personal data about an individual (e.g. letters of referral) form part of an individual's record and are maintained as part of the person's record.

vi. There are special circumstances under which disclosure of personal data to third parties is allowed. These are provided for under the Data Protection legislation and are:

- As ordered by the Garda Siochana
- For the purpose of investigating an offence
- To prevent urgent injury or damage to person or property
- Under a court order or other rule of law
- Required for the purposes of obtaining legal advice or for legal proceedings in which the person making the disclosure is a party or a witness
- Made at the request of and with the consent of the subject of the data

In all such cases, full reference will be made to the current legislation via approval by the BEST Data Protection Officer. In these additional circumstances personal information may be released without the consent of persons served under the following conditions:

- To relevant government agencies in relation to concerns regarding the health and wellbeing of minors. (See BEST's Child Protection Policy).
- To relevant health care professionals and/or designated next of kin if the person served presents with a significant risk to their own health or wellbeing (e.g. suicide risk).
- To relevant government agencies and/or health care professionals (e.g. An Garda Síochána, Psychiatric services), in situations where the person served is deemed to pose a credible threat to the health and /or wellbeing of another person (e.g. staff member, another person served, member of the public)

All of BEST's external suppliers who access BEST data must have a Service Level Agreement (SLA) in place, which includes a data protection agreement, outlining the supplier's responsibilities for any data that is shared with them. These SLAs are held in the SLA folder on SharePoint. However, BEST is ultimately still responsible for this information.

12.0 Officer responsible for implementing this Policy

The BEST Programme manager is the Data Protection Officer and is responsible for implementing this policy, including:

- Assessing BEST against the above legal requirements on an annual basis. This Self-Assessment is provided in the Appendices
- Ensuring that there are arrangements in place which support the implementation of this policy
- All staff are trained in their obligations.

13.0 Information to be provided to the Board

The DPO should report to the Board at any time where (s)he believes that Personal Data has been compromised or that the requirements of this Policy are not being met.

The DPO should provide an annual report to the board on the status of the data protection function in BEST. The Manager should provide a report to the board on data protection risk & compliance issues at least annually.

14.0 Communications Policy

In the event of a reportable and material data breach at BEST, the breach will be reported to the Board of Directors as soon possible. The Board will meet to discuss the matter and decide on an appropriate communications strategy to deal with the data breach, and the perpetrator of the breach, based on the materiality of the issue. This may involve liaison with any or all of the following stakeholders:

- Data Protection Commissioner
- Charities Regulator
- Tusla
- An Garda Síochána
- BEST's own legal advisors if necessary

The Chairperson of the Board will be responsible for communicating the breach to relevant stakeholders, potentially including BEST Clients, based on the advice of any or all of the above mentioned.

15.0 Policy Review

This policy will be reviewed every two years or when new legislation, regulatory guidelines, or the risk appetite of BEST dictates the Board to do so.

16.0 Breach of Policy

If an employee knowingly (having been made aware of the policy) breaches the policy, BEST will take the necessary corrective action in line with the Disciplinary Procedure. If a volunteer knowingly (having been made aware of the policy) breaches the policy, BEST will take all necessary corrective action in line with the Volunteer Policy.

Appendix 1 - Definition of Terms used in relation to BEST's Data Protection standards

The following technical terms are used in these Appendices:

- Data Subject – a person about whom Personal Data is processed
- Data Controller – a person or entity who collects & controls Personal Data about a Data Subject.
- Data Processor – a person or entity who processes Personal Data on behalf of a Data Controller
- Personal Data – any data, whether held in manual or automated form, which relates to a living individual. It does not have to be particularly sensitive in nature, i.e. it can be as simple as name and address
- Special categories of Personal Data - is Personal Data regarding
    - Racial origin, political, religious or philosophical views, physical or mental health, sexual orientation
- "Processing" is defined very broadly in the Act and includes
    - obtaining, recording or keeping,
    - collecting, organising, storing, altering or adapting,
    - retrieving, consulting or using,
    - disclosing the information or data by transmitting, disseminating or otherwise
    - making it available, or aligning, combining, blocking, erasing or destroying the information or data.

Appendix 2 - Data Protection Principle 1: Lawfulness, fairness, and transparency

What this principle means:

Personal Data must be obtained & processed fairly, lawfully and transparently. In order for Personal Data to be processed fairly, the Data Subjects must be informed of:

- the identity of the Data Controller
- the purpose(s) for which the data will be processed
- any other information necessary to comply with the spirit of this Act e.g. whether replies to questions are obligatory, the possible consequences of failing to reply & the existence of rights of access & rectification

Furthermore, where the Personal Data is collected other than directly from the Data Subject, (s)he must be informed of the categories of data collected from the third party as well as the name of the original Data Controller.

Where any information is likely to be used for direct marketing, the legislation requires the Data Controller to notify the Data Subject that this direct marketing will be terminated on their written request.

How BEST meets this obligation

In respect of Clients:

- The purpose of the data collected is clearly explained and makes clear that BEST is the Data Controller, for example: for application for services including clinical, accommodation and programmes
- A data register is maintained (see Table 1) which records the purpose for which data is gathered and the legal basis for processing.

In respect of staff:

- Staff employment contracts contain the necessary Data Protection disclosures.

In respect of others:

- The Manager is responsible for identifying when we collect Personal Data from other parties, why we are doing so and what notifications are necessary.

Appendix 3 - Data Protection Principle 2: Purpose Limitation

What this Principle means:
Personal Data must be kept only for specified, explicit and legitimate purpose(s). Once collected, Personal Data should be used only for the purpose(s) known to the Data Subject. Any further "secondary" use (e.g. for direct marketing) or disclosure to a third party is unlawful. The purposes should be stated in the Data Controller's registration with the Data Protection Commissioner (if applicable).
How BEST meets this obligation
The purpose for which every piece of Personal Data is collected is explained to our Clients, volunteers and Employees. A data register is maintained which records the purpose for which data is gathered and the legal basis for processing. Where BEST relies upon the consent of the individual to the processing, this consent requires affirmative action so silence, pre-ticked boxes or inactivity will be considered to be insufficient. Where the legal basis for the processing is 'consent', BEST will discontinue processing following withdrawal of that consent by the individual. The Data Protection Officer consults periodically with relevant Staff to ensure that no new information is collected other than for a specified, explicit & legitimate purpose. A Privacy Statement is published on BEST's website (BESTscp.org and has been updated to comply with GDPR standards.

Appendix 4 – Data Protection Principle 3: Data Minimisation

What this Principle means:
Personal Data must be adequate, relevant and not excessive in relation to the purpose for which they were collected.
How BEST meets this obligation
BEST annually reviews the collection of all Personal Data, whether in respect of Employees, Students, Parents, Volunteers or others to ensure that it complies with this Principle.

Appendix 5 - Data Protection Principle 4: Accuracy

What this principle means:
Personal Data must be accurate, complete and where necessary, kept up to date.
How BEST meets this obligation Areas to which this requirement is relevant include: ▪ The need to ensure that all information relating to Clients is recorded correctly. ▪ The need to ensure that a poor performance history is updated on the employee's HR file if/when (s)he improves his/her performance. The Data Protection training provided to all Staff reminds them of these obligations. Everybody is reminded of the need to update our records with any new information provided by Data Subjects, whether they be Employees or Volunteers. This might include: ▪ Change of address. ▪ Change of name on marriage. ▪ Change of marital circumstances. Employees/Volunteers have the right to delete or correct inaccurate personal data.

Appendix 6 - Data Protection Principle 5: Storage Limitation

What this Principle means:
Personal Data must not be kept for longer than is necessary
How BEST meets this obligation
BEST retains all Client records for 7 years after the relationship has ceased. Where there are other legal retention limits, then these limits apply. Detailed document retention limits are contained in the Data Register in Table 1.

Appendix 7 - Data Protection Principle 6: Integrity and Confidentiality

What this Principle means:

Personal Data must be protected against unauthorised access, alteration, disclosure or destruction, or unlawful processing

This Principle is aimed at security of Personal Data, including but not necessarily limited to:

- Physical security e.g., ensuring that hard copy Personal Data is protected by adequate security at BEST's premises.
- Electronic security e.g., network permissions, electronic theft by or other unauthorised access by employees, back-ups, hackers.
- Telephone security e.g., ensuring that all Personal Data given out over the telephone is released only to authorised recipients.

The Act also requires Data Controllers to take all reasonable steps to ensure that employees are aware of and comply with the relevant security measures in place.

How BEST meets this obligation

BEST has developed, implemented and maintained safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption/pseudonymisation/anonymisation where applicable). We will regularly evaluate and test the effectiveness of these safeguards to ensure security of our processing of personal data.

BEST Employees must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. BEST will only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

All staff must comply with all applicable aspects of BEST's Information Technology, Information Systems & Management Information, Information Systems Change Management, Information Security and Information Security Access Control policies.

All Staff are trained in:

- Physical security e.g., around the general office, filing cabinets, visibility to callers of Personal Data held on paper or on screen, disposal of paper waste.
- Electronic security - passwords, controls over rights of access & amendment, back-ups, hackers.
- Telephone security e.g., of the need to release data only to the Data Subject concerned.

Paper is shredded by 'Shred–It', a company which specialises in document destruction. Documents are shredded periodically. A certificate of confirmation of destruction is provided to BEST.

An annual review referred includes a review of each of these areas.

Appendix 8 - Data Protection Principle 7: Accountability

What this Principle means:
the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR and be able to demonstrate (through appropriate records and measures) their compliance, in particular to the DPC.
How BEST meets this obligation
As a Data Processor BEST has developed, implemented and maintained systems appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others. We will regularly evaluate and test our systems to ensure the privacy of our Data Subjects personal data. BEST Employees are trained to follow all procedures and technologies we put in place to maintain the privacy of all personal data from the point of collection to the point of destruction. All staff must are trained in and comply with all applicable aspects of BEST's Data Protection policies and procedures. An annual review is carried out annually to establish compliance with GDPR legislation which is reported to the board.

Appendix 9 – Third Party Sharing of Information

Personal Data must not be used or disclosed in a manner incompatible with those purposes. What this Principle means is that Personal Data collected by BEST must not be used or disclosed outside it except with the consent of the Data Subject or otherwise in accordance with law.
How BEST meets this obligation BEST does not disclose Personal Data to any third party except with the explicit consent of the data subject or where there is a legal obligation such as child protection concerns. All Staff are provided with Data Protection training which raises awareness of the need not to use Personal Data for any purpose other than the one for which it was provided. This reminds them of their obligation to confidentiality set out in the Data Protection Acts and the General Data Protection Regulation.

Appendix 10 - Personal Data disclosure, correction or destruction as requested by Data Subject

Subject to certain conditions, any Data Subject has the right of access, correction & erasure of Personal Data held in respect of him.
How BEST meets this obligation All Staff are trained to identify an Access Request or a request for correction or erasure. Key aspects include: 1. Although the Act requires that Access Requests must be made in writing, in the interests of Client care, if one is made verbally, we will ask the Client to make it in writing rather than simply decline it. 2. Regardless of how the request is framed, our response will include all information we hold about the Client and our response must be provided within 1 month. Where BEST receives such a request, it will be processed by the Data Protection Officer and all data held by BEST relating to the data subject will be provided including electronic, paper and CCTV within a specific timeframe if applicable.

Appendix 11 - Registration with the Data Protection Commissioner

What the law requires The Act sets out a range of types of organisations which must register under the Act.
How BEST meets this obligation BEST is not obliged to register with the Data Protection Commissioner.

Appendix 12 - Use of Data Processors

What the law requires

The legislation provides that where a Data Controller outsources part of its data processing to another party, they must

- ensure that there is a written contract in place, which obliges the Processor to comply with the instructions of the Controller and
- also provides guarantees by the Processor that he has sufficient security and organisational measures over the processing.

In addition, the Controller must take reasonable steps to ensure compliance with those measures.

How BEST meets this obligation

BEST uses the following Data Processors:

- Glitch IT

Each data processor is asked to sign a Data Processor Agreement.

Appendix 13 - Transfer of Personal Data outside the EEA

BEST does not and will not pass any Personal Data to any party outside the European Economic Area.

Appendix 14 - Personal Data Request Form

(To be completed when requesting an individual's personal data from BEST)

Personal Data Request Form

Data Protection Officer,

BEST

ADDRESS

_ _ / _ _ / _ _ _ _

Dear Sir/Madam,

I wish to make an access request under the Data Protection Acts 1988 & 2003 and the General Data Protection Regulation (2018) for a copy of any information you keep about me, on computer or in manual form. I am making this request under section 4 of the Data Protection Acts.

_____ *(signed)*

NAME (please print) _____

*ADDRESS:*_____

_____

Please Note: *Request in writing should be made and signed by the applicant in person.*

Within the terms of the Data Protection Act 1988/2003 and the General Data Protection Regulation (2018), BEST CLG will respond to your request for personal data within 30 days.

	Please check the following:	Yes	No
a)	**Completed the Access Request form in full**		
b)	**Signed and dated the Access Request Form**		

If you have ticked No to any question above, we regret we cannot process your request. Please return this form to: The Data Protection Officer, BEST Support Services CL, Office F, First Floor, Block C, The Courtyard, Newbridge, Co. Kildare

For Office Use Only.	
Regional Office:	**Regional Administration Officer:**
Regional Data Storage Location:	**Date Access Request was Received:**
Date Access Request was Completed:	

Appendix 14 - Archive Record

BEST Office Location:	
Archive Location:	
Designated Worker / Archiving:	
Please Specify the Year to be Archived:	**Number of Sheets on file:**
Date of Archiving:	
Regional Storage Address:	
Signed:	**Date:**
Please ensure that Biographical Details are stored separately	

Review Date:	**Retention Period:**
Signed:	**Date:**

Appendix 16 - Archiving - Destruction Log

BEST Office Location:
Archive Location:
Designated Archiving Person:

Year Items were Archived:
Retention Period for these Documents:
Number of Documents on file*: **Number of Documents to be destroyed*:** ***Total number of documents stored on file should accurately correspond to the total number of documents that are being destroyed***

.

I _____ *(Regional Designated Archiving Person)* declare that the following number of Documents were destroyed by me.
Total Number of documents presented for destruction:
Destruction Date: **Signed:** ***(Designated Archiving Person)***

Appendix 17 – Archives Access

Date Archive Storage Area was Accessed: **Location:**
Reason for Accessing Regional Storage Area:
Data Sought:
Has Data been removed from Regional Storage Area: **Yes: [ ] No: [ ]**
Date in which Data will be returned:
Please outline what measures will be taken to protect the integrity of this data?
Please attach the Data Subjects Access Request Form to this document.
Please do not Photocopy, Destroy or Alter any data held on file.
Signed:
Date:

Please provide a photocopy of this form to the (a) Regional Manager (b) National Data Protection Officer

Appendix 18 – Types of data held by BEST

Type of Data	Description	Location
Client Data (Student)	Student notes, outcomes	**BEST Office and Electronically**
Staff Details	Personal Details - date of birth, home telephone number, personal mobile number, home address, and next of kin. Employment Records – date of appointment, date of resignation. TOIL records, staff leave requests, training requirements and requests, staff qualifications, sickness records. Garda Vetting details.	**BEST Office and Electronically**
Community Employment Staff	None	**Held by the CE Supervisor (Not in BEST)**

Volunteer Details (Directors)	Personal Details - date of birth, home telephone number, personal mobile number, home address. Date of appointment, date of resignation. Training requirements and requests, volunteer qualifications. Garda Vetting details. ID and Proof of address.	**BEST Office and Electronically**
Mobile Phone Inventory	Details of mobile phones issued to staff which includes staff name, location, work mobile phone number.	**Electronically**
Security	CCTV cameras operate in the Geraldstown House Complex for the purpose of security and comply with BEST'S CCTV Policy.	**Electronically**
Fundraising	Personal Details - home telephone number, personal mobile number, home address. Bank Account details when donation is made by bank mandate.	**BEST Office and Electronically**

Appendix 19 – BEST Data Storage Locations

Type of Data	Storage Location And Designated Contact Person
a) Employee Data (including Contractors, Interns and Part-time Personnel) and HR Files	BEST ADDRESS And Electronically (Manager)
b) Financial Information	(MANAGER) BEST ADDRESS And Electronically
c) Client Information	(Manager) (MANAGER)
d) Historic Client Data	BEST ADDRESS And Electronically (Manager) (MANAGER) BEST ADDRESS And Electronically (Manager) (MANAGER)