DATA PROTECTION POLICY

1. Introduction

1.1 Through its day to day operations Built Environment Forum Scotland (hereafter 'BEFS') is required to collect, use and retain certain types of Personal Data about a variety of individuals. These include suppliers, current, past and prospective employees, volunteers, members and associates, potential members and others with whom it communicates. To protect the privacy of these individuals, BEFS as the Data Controller was previously required by law to comply with the General Data Protection Regulation (hereafter 'GDPR'). The GDPR was approved by the EU Parliament on 14 April 2016 and was enforceable from 25 May 2018. However, as the EU GDPR is an EU Regulation, it no longer applies to organisations operating inside the UK, who now need to comply with the Data Protection Act 2018 (DPA 2018)
To note: the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR and there is little change to the core data protection principles, rights and obligations. The GDPR continues to provide a framework of rights and duties which balance the need of organisations to collect and process Personal Data for clearly defined purposes with the right of the individuals to confidentiality. These individuals are known as Data Subjects.

1.2 This policy helps to protect BEFS and its Data Subjects from data security and privacy risks, including:
- Breaches of confidentiality. For instance, information being given out inappropriately;
- Failing to offer choice. For instance, all individuals should be free to choose how BEFS uses data relating to them;
- Reputational damage. For instance, BEFS could suffer if hackers successfully gained access to sensitive data.

1.3 Compliance with the Data Protection Act 2018 (DPA 2018) is not just a statutory obligation. BEFS regards the lawful and correct treatment of Personal Data as of vital importance to maintaining trusted and positive working relationships with the various groups of individuals whose Personal Data BEFS holds and to successful business operations.

2. Purpose

2.1 The purpose of this policy as well as related procedures and guidance is:
- to set out BEFS obligations under the UK GDPR for fair and lawful processing of Personal Data in the information created and received in the course of its activities;
- to demonstrate its commitment to, and compliance with, the UK GDPR and related legislation and standards that govern the privacy of individuals with whom BEFS has a relationship.

3. Scope

3.1 The UK GDPR relates to the processing of Personal Data. Personal Data is factual information that both identifies and relates to a living individual, and includes any expression of opinion about the individual.

3.2 The UK GDPR classifies some types of Personal Data as "Special Category" Data to which stricter conditions apply. This includes Personal Data concerning racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual orientation and criminal records.

3.3 The majority of the Personal Data held by BEFS is not part of the Special Category Data and is made up of data provided by employees and stakeholders.

3.4 The policy is applicable to all BEFS employees, volunteers, contractors, service providers and other organisations working for or on behalf of BEFS.

3.5 The policy applies to all Personal Data regardless of format or medium, including paper, electronic, audio, visual, microfilm and photographic.

4. Policy Statement and Commitment

4.1 In order to fulfil its obligations under the UK GDPR, BEFS as the Data Controller is committed to complying with the six data protection principles.

4.2 Article 5 of the UK GDPR sets out the key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.3 To comply with the UK GDPR principles, BEFS is committed to following the policy statements and related business practice, procedures, processes and systems.

4.4 BEFS is committed to privacy by design and taking a pro-active approach to privacy and data protection.

4.5 To ensure its processing of data is lawful, fair and transparent, BEFS maintains a Register of Data Processing Activities, which notes the legal basis for all data processing.

4.6 The Register of Data Processing Activities is reviewed at least annually.

5. The Rights of the Data Subject

5.1 BEFS ensures that Data Subjects can fully exercise their rights under the UK GDPR.

5.2 The UK GDPR provides the following rights for Data Subjects

5.2.1 The Right to be Informed

a) BEFS collects and processes appropriate personal information only to the extent that it is required to fulfil operational needs or to comply with any legal requirement;

b) BEFS uses privacy notices to inform the Data Subject wherever collection of Personal Data takes place, outlining the legal basis for processing, what data is collected and the purpose for processing, who it will be shared with, and how long it will be retained;

c) BEFS seeks consent from its Data Subjects when collecting Special Category Data, collecting Personal Data for unexpected or potentially objectionable purposes, processing information in a way which may significantly affect an individual, or sharing information with another organisation which would be unexpected;

d) A data protection statement is provided whenever Personal Data is gathered (for example, on a form) explaining why the data is required, and how it will be used.

5.2.2 The Right of Access

a) Subject Access Requests (hereafter 'SAR') are requests, made by the Data Subject, to access their Personal Data held by BEFS;

b) Requests for access to Personal Data should be addressed in writing or email to the Data Manager;

c) BEFS aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 calendar days unless there is a good reason for delay. In such cases, the reason for delay will be explained, in writing, to the Data Subject making the request;

d) If someone is making a request on behalf of a third party, BEFS checks that they have the authority to make that request.

5.2.3 The Right to Rectification

a) All employees who work with Personal Data will take reasonable steps to ensure it is kept as accurate and up to date as possible.
   I. BEFS will make it easy for Data Subjects to update their Personal Data;
   II. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets;
   III. Regular updates of Personal Data are carried out as specified in the Register of Data Processing Activities.

b) All employees are responsible for:

   I. checking that any Personal Data that they provide, in connection with their employment, is accurate and up to date;
   II. informing the Office Manager of any changes to their Personal Data, i.e. change of address, emergency contact; and
   III. informing the Office Manager of any errors in their Personal Data.

5.2.4 The Right to Erasure

a) BEFS retains Personal Data only for as long as it is needed for the stated purpose, through the implementation of retention policies and disposal procedures. For details, see BEFS Data Retention Policy;

b) Data Subjects have the right to have Personal Data erased or prevent further processing under certain conditions (see ICO guidance for more information). The right to erasure does not provide an absolute right to be forgotten.

5.2.5 The Right to Restrict Processing

a) Data Subjects have the right to restrict, block or supress the processing of Personal Data. When processing is restricted, BEFS is permitted to retain the Personal Data but no further processing must take place;

b) BEFS will restrict processing in the following conditions:
   I. Where the accuracy of the Personal Data is contested by the Data Subject. Processing will be restricted until the accuracy of the Personal Data has been verified;

II. Where the processing has been objected to by the Data Subject Processing will be restricted whilst BEFS considers whether the legitimate grounds override the rights of the Data Subject;
III. When the processing was unlawful and the Data Subject requests restriction rather than erasure;
IV. When BEFS no longer requires the Personal Data but the Data Subject required the Personal Data to be retained to establish, exercise or defend a legal claim.

5.2.6 The Right of Data Portability

a) Data Portability allows a Data Subject to obtain their Personal Data to reuse across different services. It allows the moving, copying or transferring of their Personal Data from one IT system to another in a safe and secure manner;

b) The right of data portability only applies:
I. to personal data a Data Subject has provided to BEFS;
II. where the legal processing condition is consent or for the performance of a contract; and
III. when the processing is carried out by automated means.

5.2.7 The Right to Object

a) Data Subjects have the right to object to processing based on legitimate interests, performance of a task in the public interest, direct marketing, profiling and for the purposes of historical or scientific research and statistics. BEFS will stop processing unless:
I. BEFS can demonstrate compelling legitimate grounds which override the rights of the Data Subject; and
II. the processing is for the establishment, exercise or defence of legal claims.

5.2.8 Rights Related to Automated Decision Making including Profiling

Data Subjects can object to potentially damaging decision being taken against them based only on automated data processing.

6. Data Security

6.1 BEFS takes appropriate technical and organisational security measures to safeguard personal information and has established information security procedures for both manual and electronic records, subject to appropriate risk assessment. These are set out in the Data Protection Policy and IT, Privacy, Security & Depreciation Policy which all employees are required to comply with and sign to acknowledge agreement.

6.2 BEFS ensures that
a) personal data stored electronically is secure, using up-to-date software;

b) access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information;

c) personal data is deleted securely, such that the data is irrecoverable;

d) appropriate back-up and disaster recovery solutions are in place.

6.3 All staff are responsible for ensuring that:

a) Any Personal Data that they hold, no matter the format, is held securely; and

b) Personal Data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

7. Data Breaches

7.1 BEFS has procedures in place to detect and respond to personal data security breaches (see Data Breach Policy). Any breaches must be reported immediately to the Director or Data Manager.

8. Data Processors

8.1 Where BEFS uses a contractor to process Personal Data on its behalf, BEFS must be satisfied that the contractor is taking adequate steps to meet its obligations as the Data Processor and allow BEFS to meet its obligations at the Data Controller under the UK GDPR.

8.2 Contracts between BEFS and the Data Processor must ensure that all necessary security procedures and other appropriate measures are specified in the contract.

9. Sharing Personal Data

9.1 BEFS will not disclose Personal Data to any third party unlawfully.

9.2 Where and when appropriate, BEFS will share information in line with the Information Commissioner's Data Sharing Code of Practice and establish Data Sharing Agreements with third parties, outlining the terms under which information will be shared.

9.3 If legally required, BEFS may release Personal Data to law enforcement agencies without the consent of the Data Subject.

10. Training

10.1 BEFS provides training for all employees in information management, security, governance and compliance, to ensure that every member of staff understands their data protection responsibilities when using Personal Data.

11. Roles and Responsibilities

11.1 All Staff

11.1.1 Compliance with this Policy is the responsibility of all BEFS employees and everyone who has access to BEFS information. Breaches of this policy and therefore the UK GDPR, whether

deliberate or through negligence, may lead to disciplinary action. A breach of the UK GDPR could also lead to criminal prosecution.

11.1.2 Colleagues must familiarise themselves with, and follow, this policy as well as the supporting policies, ensure that procedures for the collection and use of Personal Data is complied with in their area, and familiarise themselves with the implications of data protection in their job.

11.2 Director

11.2.1 BEFS is the Data Controller under the UK GDPR and the Director has senior management responsibility for ensuring that all collection and processing of Personal Data within BEFS complies with the UK GDPR and its principles.

11.3 Data Manager

11.3.1 The Data Manager is responsible for ensuring BEFS, its employees and representatives adhere to and comply with the Data Protection legislation and relevant codes of practice. They will also monitor and check compliance. More specifically the BEFS Data Manager has, but is not limited to, the following responsibilities:

a) ensuring that BEFS, its employees and representatives adhere to this policy;

b) ensuring that BEFS, its employees and representatives adhere to the six principles of the UK GDPR;

c) ensuring that BEFS employees and representatives have regular refresher courses on the data protection principles and how to apply them;

d) ensuring that all personal information is handled with respect;

e) ensuring that retained personal information is secure, relevant and not retained for any time longer than is necessary for the purpose for which it was acquired;

f) undertaking the annual data audit and review of the Register of Data Processing Activities;

g) monitoring changes to systems and documentation to ensure compliance with the Data Protection legislation and codes of practice;

h) ensuring compliance with any Subject Access Request that is received.

11.4 BEFS Board

11.4.1 The BEFS Board has the responsibility for adopting best practice as an employer and third sector body, including review and approval of Data Protection Policy and related procedures, on the recommendation of the Director and the Data Manager.

DATA RETENTION POLICY

This policy sets out the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information held by Built Environment Forum Scotland (hereafter "BEFS").

This Policy applies to BEFS employees, Trustees, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal and/or sensitive data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure compliance with it.

This policy applies to all information used within BEFS. Examples of documents include: Emails; Hard copy documents; Soft copy documents; Video and audio; Data generated by physical access control systems.

General Retention Principle
In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period will be **deemed to be 3 years from the date of creation of the document.**

General Retention Schedule
The time period for which documents and electronic records should be retained is set out in the **Data Retention Schedule**. Retention periods can be prolonged in cases such as:
When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

Destruction of Data
BEFS and its employees should, on a regular basis, review all data, whether held electronically or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant.

The data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value and their level of confidentiality. The method of disposal is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion.

The employee concerned shall perform the tasks and assume the responsibilities of destruction. The specific deletion or destruction process may be carried out by an employee or by an internal or external service provider. Any applicable provisions under relevant data protection laws and BEFS Personal Data Protection Policy shall be complied with. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

Document Disposal
Records which may be routinely destroyed, unless subject to an on-going legal or regulatory inquiry are:
Announcements and notices of day-to-day meetings and other events;
Requests for ordinary information such as travel directions;
Reservations for internal meetings without charges / external costs;

Documents such as letters, e-mails and similar items that do not add any value;
Superseded address list, distribution lists etc.;
Duplicate documents, unaltered drafts, snapshot printouts or extracts from day files;
Stock in-house publications which are obsolete or superseded; and
Trade magazines, vendor catalogues, flyers and newsletters from other external organizations.
In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.
Printed materials, including publications, newsletters, leaflets and other communications materials, should be recycled where possible.

Breaches
The Data Manager has the responsibility to ensure that BEFS complies with this Policy. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate (see BEFS Data Breach Policy for further information).

DATA BREACH POLICY

The UK General Data Protection Regulation (GDPR) imposes a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office (hereafter 'ICO'). This must occur within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individuals concerned (hereafter 'Data Subjects') must be informed without undue delay. A record of any personal data breaches must be kept, regardless of whether it is required to notify.

Policy Statement
BEFS is fully committed to compliance with the Data Protection Act 2018 (DPA 2018) specifically the UK General Data Protection Regulation (GDPR) and Privacy and Electronic Communications Regulations (PECR), and recognises its obligation to document personal data breaches and report certain types of breaches to the ICO.

Aim
This policy sets out BEFS breach detection, investigation and internal reporting procedures to meet the requirements of the aforementioned legislation. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

Definitions
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When to notify the ICO

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms needs to be established. If it is likely that there will be a risk, then the ICO needs to be notified. In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals, which include emotional distress, and physical and material damage. This should be assessed on a case by case basis. Notifiable breaches must be reported to the ICO no later than 72 hours after becoming aware of it. When reporting a breach, the GDPR states that the following information must be provided:

- a description of the nature of the personal data breach including, the categories and number of individuals concerned; and the categories and number of personal data records concerned;
- the name and contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including the measures taken to mitigate any possible adverse effects.

Notifying the ICO of a personal data breach.

When to notify the Data Subject

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Subjects concerned must be informed directly and without undue delay. The nature of the personal data breach needs to be described in clear and plain language; a contact must be named where more information can be obtained; and a description of the likely consequences and measures taken to deal with the personal data breach should be included.

Reporting an incident

All BEFS employees are responsible for reporting data breaches and information security incidents immediately to the Director and Data Manager. If the breach occurs outside working hours, it must be reported as soon as practicable. The report must include a full description of the incident, when it occurred, who is reporting it, what personal data was breached and how many Data Subjects are involved. The reporting individual must complete an entry in the Personal Data Security Breach Log.

Containment and risk assessment

The Director in liaison with the Data Manager will conduct an initial assessment of the severity of the breach, and establish who may need to be notified as part of the initial containment, and inform the police, where appropriate. The Data Manger will investigate whether there is anything that can be done to recover or limit the damage of the breach. They will also assess the risks associated with it and any adverse consequences for individuals, specifically whether there is a high risk of affecting individuals' rights and freedoms under Data Protection legislation.

Notification

BEFS Director, in consultation with the Data Manager, will establish whether the Information Commissioner's Office needs to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible; and whether the Data Subjects concerned need to be notified.

Evaluation

Once the initial incident is contained, the Data Manager will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes need to be made to systems, policies and procedures.