



Privacy and Personal Data Protection Policy

Document Ref.	ESSPPDPP
Version:	10
Dated:	16 October 2024
Document Author:	Nick Yoxall
Document Owner:	Catherine Storer

Revision History


Next planned review date
15/10/2024

Version	Date	Revision Author	Summary of Changes
2	26 November 2018	E Proctor	Including Digital and Video images
3	22 March 2019	E Proctor	Policy Review
4	22 August 2019	A Volante	Update to include - This policy is applied to all aspects of the delivery of ESF projects
5	08.11.2019	A Volante	Amendment to Document Reference
6	08/11/2020	N Yoxall	Document Review
7	08/10/2021	N Yoxall	Reference to Staff Training (2.11) GDPR & Data Protection Legislation
8	04/10/2022	N Yoxall	Document Review
9	13/10/2023	N Yoxall	Annual Review – Document Ref Change
10	16/10/2024	N Yoxall	Annual Review <ul style="list-style-type: none"> • Updated Gov.uk hyperlink • Training reference changed from OneFile to BrightHR • Ref to GDPR changed to DPA 2018 (GDPR) throughout

Distribution

Name	Title
All Employees	Privacy and Personal Data Protection Policy
All Stakeholders and External Parties	Privacy and Personal Data Protection Policy

Approval

Name	Position	Signature	Date
Catherine Storer	Executive Director		16/10/2024

Contents

1	INTRODUCTION.....	3
2	PRIVACY AND PERSONAL DATA PROTECTION POLICY	4
2.1	THE DATA PROTECTION ACT 2018.....	4
2.2	DEFINITIONS.....	4
2.3	PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA	5
2.4	RIGHTS OF THE INDIVIDUAL	6
2.5	CONSENT.....	7
2.6	PRIVACY BY DESIGN	7
2.7	TRANSFER OF PERSONAL DATA.....	7
2.8	DATA PROTECTION OFFICER	8
2.9	BREACH NOTIFICATION.....	8
2.10	ADDRESSING COMPLIANCE TO THE DPA 2018.....	8
2.11	TRAINING	9
3	DIGITAL AND VIDEO IMAGES.....	9

1 Introduction

In its everyday business operations Essential Site Skills makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Essential Site Skills is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Essential Site Skills systems.

2 Privacy and Personal Data Protection Policy

2.1 The Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'.

They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation
-

There are separate safeguards for personal data relating to criminal convictions and offences. It is Essential Site Skills policy to ensure that our compliance with the DPA 2018 (GDPR) and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

There are a total of 26 definitions listed within the DPA 2018 and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means:

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the DPA 2018 is based.

These are as follows:

1. *Personal data shall be:*

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('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, in accordance with Article 89(1), 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('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').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Essential Site Skills must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

2.4 Rights of the Individual

The data subject also has rights under the DPA 2018. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Essential Site Skills that allow the required action to be taken within the timescales stated in the DPA 2018.

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection

Rights in relation to automated decision making and profiling.	Not specified
--	---------------

Table 1 - Timescales for data subject requests

2.5 Consent

Unless it is necessary for a reason allowable in the DPA 2018, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

2.6 Privacy by Design

Essential Site Skills has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimisation and pseudonymisation should be considered where applicable and appropriate.

2.7 Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the DPA 2018. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

2.8 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the DPA 2018 if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Essential Site Skills requires a Data Protection Officer to be appointed.

2.9 Breach Notification

It is Essential Site Skills policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the DPA 2018, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the DPA 2018 the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

2.10 Addressing Compliance to the DPA 2018

The following actions are undertaken to ensure that Essential Site Skills complies at all times with the accountability principle of DPA 2018:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
 - Organisation name and relevant details

- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

Further information can be found here [Print Data protection: The Data Protection Act - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/consultations/print-data-protection-the-data-protection-act)

2.11 Training

All employees are enrolled on our DPA Training via BrightHR the online Data Protection course is designed to help businesses and individuals comply with the essential principles of the Data Protection Act and the EU and UK General Data Protection Regulation (GDPR) and heighten awareness regarding compliance. All Staff must successfully complete the programme, with 100% required in order to successfully complete the course. This is updated to reflect any changes to legislation (and reissued where required) and in addition an annual review of content prior to requests sent for completion.

3 Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Essential Site Skills will inform and educate users about these risks and have implemented policies to reduce the likelihood of the potential for harm (see Acceptable Use Policy and Staff Code of Conduct):

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images, using Essential Site Skills equipment only, to support educational aims, but must follow Essential Site Skills policies concerning the sharing, distribution and publication of those images.

- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or Essential Site Skills into disrepute
- Learners must not take, use, share, publish or distribute images of others (staff and learners) without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice on the use of such images
- Learners full names will not be used anywhere on a website or blog, particularly in association with photographs unless consent has been given
- Written permission from parents or carers will be obtained before photographs of learners are published on the website or for other promotional
- Cameras and mobile phones are prohibited in the toilet areas
- Visitors, volunteers and learners are not permitted to use their own mobile phones to take or record any images of other learners at any time, unless authorisation is given by Essential Site Skills and learner/s.