



Data Protection/Data Management Policy

Introduction

Flynn's Barn needs to keep certain information about young people who use the charity's services, and its own employees and volunteers, to allow it to manage the charity, and monitor its performance, and to operate effectively. It is also necessary to process information so that staff can be recruited and paid, so that services can be organised and various legal obligations to government bodies (eg HMRC and charity commission) can be complied with.

To comply with legislation, information must be collected and used fairly, stored securely and not disclosed to any person unlawfully. To do this, we must comply with the principles set out in the General Data Protection Regulation (GDPR), tailored by the Data Protection Act 2018.

Protecting the confidentiality and integrity of personal data is a key responsibility of everyone at Flynn's Barn and our staff and volunteers are obliged to comply with this policy at all times to minimise the potential risk of damage and distress to Individuals and also the risk of penalties, fines, legal action and reputational damage to the charity. Failure to comply with this policy could result in disciplinary action and/or any other action Flynn's Barn deems necessary.

Policy Statement

We will ensure that all personal data is processed fairly and lawfully, including under the requirements of GDPR.

We have a nominated Data Protection Officer (who also fulfils the role of Data Controller) who can be contacted at info@flynnesbarn.org or by calling 01768 800 686

The following lawful purposes for processing ordinary Personal Data as set out in Article 6 of the GDPR and are as follows (paraphrased):

- the use of the Personal Data for the purposes of the legitimate interests of Flynn's Barn in the provision of its services
- the processing is necessary for the performance of a contract
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary in order to protect the vital interests of the individual or of another natural person (eg health & safety or safeguarding);
- the processing is necessary for the performance of a task carried out in the public interest; and
- the individual who is the subject of the Personal Data has given consent for one or more specific purposes.

Most data held by Flynn's Barn uses the legal basis of legitimate interest and relies on consent only as a last resort.

Key Definitions

Controller – Any entity (eg company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data i.e. Flynne's Barn

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Acts of 1998 and 2018.

Data Protection Officer – Our Data Protection Officer can be contacted at info@flynnesbarn.org or by calling 01768 800 686

Personal Data – Any information about an Individual which identifies them or allows them to be identified in conjunction with other information that is held.

Personal data is defined broadly and covers things such as name, address, email address, IP address and also more sensitive types of data such as genetic data and religious beliefs.

Processor – Any entity (eg company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include, where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services. Wherever personal data is processed on the authority of the controller, a data sharing agreement is put in place to provide assurance on the security of the data.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data (i.e., information about their inherited or acquired genetic characteristics), biometric data (i.e., information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

General Data Protection Regulation Principles

When using Personal Data, Data Protection Laws require that we comply with the following principles that require Personal Data to be:

- a. processed lawfully, fairly and in a transparent manner.
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- c. adequate, relevant and limited to what is necessary for the purposes for which it is being processed.
- d. accurate and kept up to date, meaning that every reasonable step must be taken to ensure Personal Data that is inaccurate is erased or rectified as soon as possible.
- e. kept for no longer than is necessary for the purposes for which it is being processed.
- 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.

Responsibilities of staff

All Flynnne's Barn employees must comply with this policy and ensure they never release or disclose personal information to others who are not authorised to access personal data. All our employees must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties

All staff are responsible for:

- checking that their own personal information provided to Flynnne's Barn in connection with their employment is accurate and up to date

If, and when, as part of their responsibilities, staff collect information on others (i.e.. young people accessing Flynnne's Barn services), they must comply with all procedures on the management of personal data. This includes the following key practices:

- a. Adopting the concept of "tidy desk" whereby there is no risk of personal data being inadvertently shared.
- b. Locking away all personal data when not at your desk
- c. Never leaving your desktop or laptop open when away from your desk
- d. Ensuring that no data is transferred outside Flynnne's Barn without appropriate security measures being applied such as data encryption and two-factor authentication
- e. Checking if a data sharing agreement is in place when data needs to be shared with another processing organisation

The Data Protection Officer is responsible for:

Keeping this policy updated and relevant

Ensuring that Flynnne's Barn complies with the Data Protection Acts 1998/2018 including the General Data Protection Regulation

Ensuring that relevant and appropriate training is held when inducting new staff

Marketing and Consent

Flynnne's Barn will sometimes contact Individuals to send them marketing materials or to promote the charity. Where Flynnne's Barn carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR requires a number of important changes for organisations that market to individuals, including:

- Providing more detail in their privacy notices, including for example whether profiling takes place
- Rules on obtaining consent are stricter and will require an individual's "clear affirmative action"

Consent is central to electronic marketing. Best practice is to provide an un-ticked opt-in box.

Data Protection Impact Assessments (DPIA)

The GDPR introduced a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- a. describe the collection and use of Personal Data.
- b. assess its necessity and its proportionality in relation to the purposes.
- c. assess the risks to the rights and freedoms of individuals; and
- d. the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. Where a DPIA reveals risks which are not appropriately mitigated, the ICO must be consulted. All DPIAs must be reviewed and approved by the Data Protection Officer.

Subject Access Request (SAR)

A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which Flynn's Barn holds about them. We will normally respond to SARs within one month of a request (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). All subject access requests received must be forwarded to the Data Protection Officer can be contacted at info@flynnesbarn.org or by calling 01768 800 686

We do not charge a fee for the handling of normal SARs. The Charity reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive

Appendix 1 - Lawful Processing of Personal Data

Flynne's Barn will ensure that the collection and use of personal data is lawful, this means that any use of 'personal data' must fall within a "lawful purpose"

Contractual Obligation: The processing is necessary for a contract we have with an individual or third party or specific steps we are asked to take before entering into a contract eg Terms and conditions of employment/Payroll Info/ and supplying goods and services to organisations.

Legal Obligation: The processing is necessary for Flynne's Barn to comply with the law (not including contractual obligations). There are many lawful obligations which we must fulfil eg Tax/Pension/Compliance with Health & Safety at Work Act/Equality & Diversity. We must process personal data lawfully if the data processing falls within this category.

Vital Interest: The processing is necessary to protect someone's life and includes emergency information eg in cases of life or death

Legitimate Interest: The processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the Individual's personal data which overrides those legitimate interests.

Consent: The Individual has given clear consent for Flynne's Barn to process their personal data for one or more specific purposes.

Consent must be:

- Freely given
- People Specific
- A form of firm confirmation or positive opt-in, such as ticking boxes on a webpage
- Easily able to be withdrawn

Consent cannot be obtained from the following:

- Silence
- Pre-ticked boxes
- An unambiguous indication of an individual's (data subjects) wishes
- Inactivity

Lawful purposes for processing 'Special Categories of Personal Data'

There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 of the GDPR and are as follows (paraphrased):

- Explicit consent
- Employment and social security obligations
- Vital interests
- Necessary for establishment or defence of legal claims
- Substantial public interest
- Various scientific and medical issues.