FWinc Data Protection & Confidentiality Policy

Funny Wonders Inc.
Community Interest Company
Company No: 06814964

1. Purpose

Funny Wonders Inc. (FWinc), as an organisation, aims to provide opportunities for people to experience and participate in creative arts in a supportive, safe environment. In order to operate efficiently, FWinc is required to collect, use and hold use certain types of information to contact and communicate with its members and associates and in case of emergency, medical or otherwise. In addition, we may be required, by law, to collect and use certain types of information to comply with statutory obligations.

This policy addresses the issues surrounding data protection and confidentiality regarding personal and private information including contact details, medical conditions, evaluation forms, complaints, safeguarding and other issues of a sensitive nature. The purpose of this policy is to aid FWinc to comply with legislation, provide practical guidelines for FWinc members and associates and to create a safe environment where individuals are treated with respect.

2. Scope

This Policy applies to all members and associates of FWinc; especially strategic (Directors), operational (project managers) and delivery (activity team) personnel.

3. Definitions

Personal data is defined as any information relating to a person who can be directly or indirectly identified (for example, by reference to an identifier such as a number or online handle) and which is held in an organised filing system. It includes personal information (e.g. name, date of birth, location), consents, medical information and information relating to sensitive issues (e.g. special categories or genetic/biometric data). There is an expectation of confidentiality with any personal data entrusted to a second party - that it will be kept private and not made available to the public.

High-risk or special categories of personal data is more sensitive and defined as that which may cause discrimination, damage to reputation, identity theft, financial loss, loss of confidentiality or any other significant economic or social disadvantage and which may create risks to an individual's fundamental rights and freedoms. It includes ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation and activity and biometric, genetic and health data.

Processing broadly means collecting, using, disclosing, retaining or disposing of personal data.

A controller is an organisation which determines the purposes and means of processing personal data, decides what data is collected, how it is used, stored and any security measures.

A processor is an organisation responsible for processing personal data. It may be a third party acting on behalf of a controller. A processor may become a controller if they add to the data, before giving it back to the controller.

A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is more than just losing personal data.

The FWinc electronic database comprises of Microsoft Excel files with spreadsheets containing electronic versions of personal data obtained from registration forms and public contact details of businesses and organisations. It is held on the FWinc laptop and any back-up devices.

A "safe and secure" location infers one which is private, locked or lockable, inaccessible to the public and safe from damage (e.g. flooding).

4. Statement of Data Protection and Confidentiality

FWinc regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. FWinc will make steps to ensure that the organisation treats personal information lawfully, fairly and correctly and will deal with personal data properly, whether on paper or in electronic form, and will comply with government legislation. FWinc recognises that it is responsible and accountable for the protection of the personal data which it holds. FWinc offers confidentiality and will preserve and maintain the confidentiality of information we receive.

FWinc aims to hold all personal data collected in an organised filing system in both hardware and digital formats and is therefore subject to data protection legislation. Whilst personal data yet to be filed is not subject to such, FWinc aims to operate under best practice and will do its due diligence.

5. Legislation

5.1 Human Rights Act 1998
Article 8 of this Act states that everyone has a right to respect for their private and family life, home and correspondence. Authorities must not interfere with this right except where the law permits them to and when it is necessary in a democratic society.

5.2 Common Duty of Confidence
This is a common law (not an Act of Parliament). It recognises that those providing information have an expectation that it will not be shared or disclosed to others. Information should only be disclosed with consent, if there is enough robust public interest justification (such as the protection of children or vulnerable adults, prevention or detection of crime or ensuring public safety) or required by statute.

5.3 Data Protection Act (DPA) 1998
This Act made new provisions for the regulation of the processing of information relating to individuals, including facts and opinions about an individual which might identify them; and concerns the obtaining, holding, use or disclosure of such information. The DPA ensures that information held about any person cannot be used for purposes other than those for which it was originally supplied, without the person's consent. It also enables an individual to request to know the information held about themselves and gives them have the right to receive copies of this information and order it to be destroyed.

There are eight protection principles of this Act. Information must be:

1. obtained and processed fairly and lawfully
2. held only for specified and lawful purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the DPA and an individual's rights
7. kept secure
8. transferred in accordance with these principles

For more information of these principles, see Appendix A.

5.4 Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003
Regulations derived from EU law for organisations that wish to send electronic marketing messages (by phone, fax, email or text), use cookies, or provide electronic communication services to the public. They sit alongside the Data Protection Act, setting out some extra rules for electronic communications and give people specific privacy rights regarding traffic and location data, itemised billing, line identification, and directory listings. They have been amended in 2004, 2011, 2015 and 2016. See the FWinc Online Policy for more information.

5.5 General Data Protection Regulation (GDPR) 2018
The GDPR is an extension of the DPA 1998. Every organisation that processes personal data within the EU (or outside the EU that offer goods or services to individuals in the EU) must be compliant with new GDPR by 25th May 2018 including charities and voluntary organisations. The GDPR enables

Member States to introduce derogations in certain situations but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society. They apply to both digital and manual filing systems but not to certain activities covered by the Law Enforcement Directive, processing for national security purposes or processing carried out by individuals purely for personal/household activities.

The GDPR aims to create a culture of privacy, transparency, accountability and governance throughout organisations. They give specific new obligations for how organisations handle personal data in order to prevent fraud and the illegal use of data. They clarify who is accountable for what in order to stop blame and finger pointing. They update the approach to processing personal data, create some new rights for individuals and strengthen some rights which currently exist including increased understanding, protection (particularly for children) and mitigation against the risk created for individuals in exchange for using their personal data. They also set a high standard for consent.

The main responsibilities of organisations are outlined in the following data protection principles. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. 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.
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR provides the following rights for individuals:

- to be informed
- to access
- to rectification
- to erasure or to be forgotten
- to restrict processing
- to data portability
- to object
- relating to automated decision making and profiling.

For more information on these rights, see Appendix B.

To see what other changes are introduced by the GDPR, please see Appendix C. The Information Commissioner's Office (ICO) will look to work with organisations to gain GDPR compliance if they can show to be trying and taking all reasonable steps. Fines will be given to those blatantly disregarding the new regulations and ignoring the authorities.

6. Data Protection Officer

DPO is an official term for a worker formally and legally responsible for data protection procedure and policy within or for an organisation. According to the GDPR, FWinc does not legally require a DPO. In order to avoid confusion, the member of the FWinc team who undertakes the work of the DPO will be referred to as the FWinc Data Lead (FWincDL).

7. FWinc Activities and Projects - Privacy By Design

'Privacy by design' is an approach to projects that promotes privacy and data protection compliance from the start. Activities and projects planned by FWinc should consider data protection and confidentiality at every stage of project management and as such should be included in the FWinc Project Management Guidelines.

Data protection impact assessments (DPIAs) should be incorporated into project, event, activity and venue risk assessments. DPIAs should include: an assessment of the necessity of the processing operations and proportionality in relation to that purpose; assessment of the risks to the individual; the measures in place to address the risk; risks associated with obtaining, using and storing personal data.

Identified risks include: security of FWinc project folders; laptop accessibility; online accessibility; and electronic device accessibility. Security measures should be in place to protect from data breaches: see section 13 for how to store personal data.

Reviews of FWinc consent processes should be carried out at the beginning of each major project (for which project management documents are produced) and consider any new risks due to the project design.

To aid evaluation of FWinc data protection procedures and transparency, the FWincDL should map the journey of personal data through the organisation. This should incorporate a timeline and any third parties. Identified data sources include: registration forms, emails and feedback forms.

Data protection procedures should also be evaluated and included in evaluation reports to aid continuous improvement across FWinc projects. As such, data protection should be included in the FWinc Evaluation Report template.

8. Obtaining Personal Data

8.1 Lawful Basis

The lawful basis under which FWinc is able to collect personal data is by obtaining consent from those providing it. Those giving consent on behalf of a child must be a person holding 'parental responsibility'. A record should be kept of when and how consent is given and by whom.

8.2 Data Subjects

FWinc obtains personal data from:

- directors of the company
- team members including paid workers and volunteers
- youth members
- workshop participants

For workshop participants and youth members, the provision of this information is not necessary to participate in FWinc activities and consents for FWinc to hold it can be declined or withdrawn without detriment. The provision of this information, however, is necessary to become a director of FWinc or a member of the FWinc Team for reasons of safeguarding.

FWinc also obtains publicly-available data from the internet or local media. The source of this data and date of collection, if not provided by a data subject, should be recorded in the FWinc Database. Publicly-available data has an 'expectation of use' such as contact regarding relevant activities or issues. FWinc should not add such data to its mailing lists or send irrelevant or unexpected communication without first obtaining consent.

8.3 Personal Data of Children

Once a young person becomes 18, they have the 'right to be forgotten' for personal data before they were 18. Upon turning 18, FWinc should endeavour to re-obtain their personal data and consent using adult versions of relevant forms.

8.4 Purpose of Personal Data Collection

The specific purpose for the collection of all personal data should be stated and its use justified to ensure it is legitimate (see section 9). As little personal data should be collected as necessary for the safe operation of activities.

Personal data collected by FWinc will not be used for any purpose other than those stated in the privacy statement.

8.5 Privacy Statement

All data subjects providing personal data to FWinc should be provided with a privacy statement detailing what happens to their data. To ensure transparency and accessibility, this statement should be clearly available on the FWinc website (for reference) and a copy given to anyone filling in registration forms to retain for their information.

The privacy statement should state, in a comprehensible, concise and clear way (so that a child may understand it):

- why FWinc is collecting their data
- that the data is for Funny Wonders Inc. and will not be passed on to any third party
- under what lawful basis FWinc is able to collect their data
- whether the provision of personal data is part of a statutory/contractual requirement or obligation and possible consequences of failing to provide the personal data OR the option to not provide personal data without detriment
- how their data will be used
- what will be sent to them
- how their data will be stored
- for how long their data will be retained/stored
- the criteria used to determine the retention period
- if their data will be shared
- the legitimate interest of any third parties, controllers or processors
- how/if their data will be processed and the types of processing activity
- the existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences
- how they can request to know what data is held
- how they can unsubscribe from mailing lists
- how they may request their data be deleted, including FWinc contact information
- who has the responsibility for handling their data, including their contact information
- that their data will be held in accordance with the Data Protection Act 1998
- the existence of their rights including the right to withdraw their consent, object or to lodge a complaint with a supervisory authority. Their right to object must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

See Appendix D for a Privacy Statement template.

8.6 Positive, Opt-in Consent

To obtain consent for specific actions, following the privacy statement, FWinc forms should have clear, granular questions with unfilled tick boxes. See Appendix D for a template.

Verbal consents may be given, but these should be recorded and every effort should be made to obtain written consent.

Consents obtained from FWinc forms, prior to 25th May 2018, which are not GDPR-compliant, should be re-obtained. Every effort must be made to re-contact data subjects for opt-in consents which were not clarified or specified previously or not from a positively opt-in method.

9. Relevant Personal Data

All personal data held by FWinc is given directly from FWinc members and associates or parents/guardians of U18 FWinc members and associates.

9.1 Personal Information

FWinc obtains personal information of members and associates (including workers, volunteers, supporters, workshop participants and professional artists) in order to contact them regarding FWinc activities. This information includes: name, birthday, gender, address, phone numbers, email addresses, emergency contacts, referee contacts.

We obtain birthdays to determine the age of participants and to be aware of any birthdays, particularly of young participants. It will not be used to raise funds for FWinc or any other cause or organisation. We obtain gender to aid referencing individuals and identification.

Named business email addresses of public organisations, such as teacher's school email addresses, are assumed to be publicly available and held on the FWinc contacts database without consent. Those of private companies which are not publicly available or published should be collected with consent.

It is assumed consent to hold personal data not received from the data subject i.e. emergency contacts' and referees' details, is given by proxy; reasonably assuming that the person giving the data has obtained their consent to be an emergency contact or referee. Such data subjects have the right

to know the source from which their data originated. FWinc Team members should explain how they have their personal data when the first communication takes place. FWinc should only use this information for that which it was intended and not for marketing purposes.

9.2 Further Personal Information

Further personal data such as identification information/document numbers, previous addresses and National Insurance Numbers are obtained to carry out DBS checks during recruitment, however, this information is not, and should not be, recorded or kept by FWinc.

Bank account information is often present on the invoices of FWinc workers or associates and consequently held on computers in appropriate financial folders and online in association with the FWinc bank account. These details are not, and should not be, copied into any electronic or hard-copy database by FWinc. Any computer used by FWinc members, which holds such information, should be secure with user passwords and appropriate anti-virus software. FWinc relies on its bank having sufficient data security measures to maintain privacy. FWinc should do its due diligence to ensure its bank is GDPR-compliant: see section 18.2.

9.3 Activity Consent

FWinc obtains information regarding consent for participation, photography and video, breaks, evaluation and medical issues which may reveal sensitive information such as religious beliefs or medical conditions. This information will be held on the electronic database and on either hard-copy or electronic Consent forms.

This information is required by FWinc for safety reasons, particularly if an adult, responsible for an U18 participant is not present at the activity or a person is a regular participant at FWinc activities. For one-off participants or first time participants at FWinc activities, verbal consents may be given, particularly if an adult responsible for an U18 is not present during the activity. Every effort must be made to acquire the information at later sessions.

9.4 Medical Conditions

FWinc require information on any medical conditions which may affect themselves or other members and associates of FWinc which FWinc may need to deal with during FWinc activities or any administration of medicine which needs to occur during FWinc activities. This information will be held on the electronic database and on Membership Registration, Contact Details, Application or Medical Administration forms. FWinc supervising adults will be informed of persons with medical conditions when thought necessary by the FWinc Wellbeing Officer (FWincWO) and those involved or parents/guardians/carers of under-18s. Supervising adults will receive any necessary training on how to manage the condition(s) and what action may be required.

9.5 Sensitive Issues

When dealing with sensitive issues, such as a disclosure of abuse or neglect, no member or associate of FWinc should state they will maintain confidentiality or that they will not relate information to anyone in order to get the affected person to reveal their issue: all such disclosures must be reported and it is important not to make and break promises. The fact they have mentioned something already suggests they want to talk about it. All disclosures should be handled in accordance with the FWinc Safeguarding Policy with information and relevant personal data shared with role-specific people.

9.6 Evaluation Forms

FWinc obtains opinions of our activities on Evaluation Forms. These can be completed anonymously and do not request any personal data other than opinions.

FWinc intends for evaluation forms to be handled by an independent evaluator who will not be directly involved with FWinc activities. If this is not possible or necessary, forms will be handled by the FWinc Administrative Assistant (FWincAA). Only the FWincAA will have access to paper copies or emails with attached feedback forms. Evaluation data will be reported to the FWinc Board of Directors upholding anonymity.

10. Processing of Personal Data

FWinc will not pass personal data to a processor. Any processing of personal data which is required, including financial processing, will be carried out by FWinc. The lawful basis under which FWinc can process personal data is by obtaining consent of the data subject.

FWinc will process personal data provided on forms into the FWinc electronic database to maintain a record of our activities and participants. FWinc will further process personal data for statistical and evaluation purposes relating to activity participation and include information relating to: location, age, frequency of participation.

Whilst using and processing data, FWinc should continue to ensure the safety and security of personal data. This includes: ensuring no public access whilst handling hardware copies; locking electronic devices or logging off user platforms whilst away from them; project folders present at activities are kept away from participants and monitored at all times; computer screens are kept away from windows.

11. Sharing Personal Data

Personal data will be shared within FWinc on a need-to-know basis only; for example, if the person receiving the information is concerned with contacting an individual or gaining information regarding FWinc activities; or in order to provide the best service to our members and associates.

During general, day-to-day activities, FWinc will not share personal data with third parties except in circumstances where it is necessary (see section 14). FWinc uses services by other companies which may have access to digital personal data as part of their service. FWinc will do its due-diligence to ensure these companies are GDPR-compliant (see section 18.2).

Should FWinc need to share personal data, we will obtain implicit consent from the data subject to do so; for example, if any project involves travel or accommodation and relevant information is required during booking and/or payment. If data is shared to a third party it will be recorded and explained on the FWinc electronic database.

12. Retention of Personal Data

FWinc will keep the personal data of it members and associates for a maximum of twenty years following last participation or contact.

FWinc is justified to retain data for this duration due to the infrequency of our activities and large projects: we also do not want any cause to exclude past participants who may like to get back involved. We also want to be able to invite past participants to periodic anniversaries and celebration events.

13. Storage of Personal Data

FWinc aims to store personal data in a safe and secure environment but which also must be easily locatable and accessible for those who need access; such as the FWincDL when handling requests or project managers needing to communicate with participants.

FWinc members in possession of personal data should mitigate against the risk of damage, loss or theft in risk assessments. Any queries regarding the storage of confidential information should contact the FWincDL.

Any data held of a particularly sensitive nature (e.g. medical conditions, criminal convictions, personal safety, financial information) should be split from the main record and kept in a separate location under a pseudonym or identifier referred to in the main record.

The personal data of FWinc members or associates should not be held in personal books/databases unless personal relationships are established outside of FWinc activities.

13.1 Hardware (Paper) Versions

Hardware (paper) versions of confidential information should be held in a closed, storage unit in a safe and secure environment managed by the FWincDL.

Hardware versions must not be transported in any unsecure manner. Forms held in workshop folders at FWinc activities should be kept away from participants and never left unattended. Activities where folders are present, should have registers taken so the attendance can be known determined in any investigation, should there be a breach.

13.2 Electronic Versions

Personal data given on hard-copy or electronically will be compiled into the FWinc electronic database. This should also record when and how consent was given, by whom and make clear if any consents were not given.

The electronic database should be held on a password-protected computer with suitable firewall and anti-virus protection and on an encrypted hard-drive. It should not be held in shared folders and therefore accessible to guest or other users. Any hardware copies of data must be kept in a separate, safe and secure location. Any electronic back-ups of data on portable or external devices must be kept in a safe and secure location, password protected and encrypted (enable BitLocker in device settings). When disposing of computers and devices, all personal data must be completely removed from the hard-drive and recycle bin.

Portable devices (e.g. tablets, phones) containing or with access to FWinc personal data (including email addresses) should be contained in a safe and secure environment and be password-protected. Any theft of such items must be recorded with FWinc and individuals informed of the theft. When disposing of devices, all personal data must be completely removed.

Passwords should be secure i.e. difficult to guess or work out, and changed regularly. They should contain upper and lower case letters, numbers and, where permitted, punctuation marks. It is better to write down and hide a complex password than use simple ones. Passwords for online sites should not be remembered by computers. See the FWinc Online Policy for more information on cyber-security.

Confidential information must not be uploaded onto the internet nor sent in emails. Group emails sent by FWinc members and associates to members of the public should utilise the blind carbon copy (bcc) tool in order to hide the email addresses of all the recipients unless communication between all is required (e.g. between the FWinc team).

14. Disclosure

The police have no automatic right to confidential information however confidential information can be disclosed in the following circumstances:

- with the individual's written, informed, explicit consent for a particular purpose: individuals over 18 are regarded as adults by FWinc and must be asked directly for consent to disclose information; a parent/guardian/carer must be asked those under 18.
- if it is required by law, to comply with the law, including civil law, or under a court order
- if it is regarding safeguarding and the protection of a child or vulnerable adult
- to safeguard national security, defence, public security, public interest (particularly economic or financial) or public health including monitoring, inspecting or regulating functions
- over suspected terrorist activity in accordance with the Terrorism Act 2000
- to prevent, investigate, detect or prosecute criminal offences including money-laundering, drug trafficking, acts of treason
- to protect judicial independence and proceedings
- to prevent breaches of ethics in regulated professions
- to protect the individual or rights and freedoms of others

In such circumstances, the information will only be passed on as permitted in this Policy and following confirmation from the FWincDL. FWinc must be able to justify any decision to pass on information: notes must be taken regarding any such decisions. Wherever possible and appropriate, the person will be informed that this action has been taken.

For disclosures of personal data for reasons other than those circumstances stated above, FWinc will seek permission or provide contact details to the individuals so they may choose whether or not to disclose their personal data to another organisation. Disclosures, in exceptional circumstances, may be justified, if in the individual's best interests, but where none of the statutory exemptions apply.

As an organisation operating within the public domain, FWinc requires public contact details including of the registered office. FWinc will only show FWinc email addresses in the public domain, and preferably not person-specific email addresses. FWinc aims to not publicise phone numbers in promotional materials

but this may not be realistic considering its commitment to advertise using various methods and able to be contacted by those who do not use email.

15. Subject Access Requests (SARs)

Any SARs received by any FWinc team member or FWinc Director should be given to the FWincDL. The FWincDL should respond to the requestee in a prompt manner and definitely within one month and fulfil any request in accordance with the GDPR 2018. As such, FWinc may: refuse to respond to a request if it is manifestly unfounded or excessive; charge a reasonable administration fee **for** dealing with the request.

FWinc should ensure all personal data held is easily accessible in order to promptly address any SAR.

As the GDPR require data processing actions to be recorded, FWinc will keep a record of those who have submitted an SAR and the action taken by FWinc.

16. Deletion of Personal Data

The deletion of personal data, upon request, should be managed by the FWincDL. The FWincDL should respond to the requestee in a prompt manner and definitely within one month.

If the FWincDL determines the personal data should be deleted, they should communicate what is to be deleted and within what time-frame to the FWinc Team.

Digital personal data should be deleted from all electronic devices (e.g. laptop, external hard-drive, pen drives, phones) including all back-ups and copies, from email contacts of all FWinc email accounts. Emails between only the requestee and FWinc email accounts should be deleted and emptied from any trash/deleted folders. Emails between other recipients may contain important or relevant information and therefore, should not be automatically deleted. If from a past or present team member, their mention on the FWinc website should also be deleted if requested.

All hardware copies of their personal data (e.g. registration forms, database print-outs) should be destroyed - shredded or burnt.

As GDPR require data processing actions to be recorded, FWinc will keep a record of those who have their data deleted. This record will contain minimal personal data and use an identifier where appropriate.

17. Data Breaches and Misconduct Regarding Data Protection and Confidentiality

Persons who breach this Policy or the law or those who try to access confidential information will be subject to the FWinc Disciplinary Procedure outlined in the FWinc Disciplinary Policy. Any data breach or attempt should be reported using a FWinc Record of Misconduct Report Form. All data breaches will be investigated by the FWincDL with the breach contained, recovered, risk of further breaches assessed and measures taken to reduce this risk.

Should any data breach be deemed serious, criminal or likely to result in a risk to the rights or freedoms of an individual, as assessed in a DPIA, the occurrence should be reported to the ICO and to the individuals involved, when appropriate. This should occur within 72hrs of it being discovered. There is little case law to guide when breaches should be reported: it is recommended to err on the side of caution. Notifications can be made online.

Data breach notifications should include: the nature of the breach; the number of individuals concerned; special categories of individuals concerned; what has been taken or potential range if not known; how it happened; the name and contact information of the FWincDL or other contact point; a description of the potential consequences of the data breach (depending upon the type of data breached); a description of the measures taken or proposed to deal with the data breach and its effects; and a description of the measures planned to mitigate against future data breaches.

18. Compliance and Accountability

In order to demonstrate compliance with the principles of the GDPR and to operate under a climate of best practice, FWinc should take the following steps:

1. Appoint a Data Controller so that our procedures and responsibilities are clear.
2. Use tools provided by the ICO to ensure GDPR-compliance.
3. Attend training regarding data protection and research security measures.
4. Audit the personal data already held and document its processing.
5. Amend privacy notices and consent requests on FWinc forms.
6. Draw attention to and explain procedures within the FWinc Data Protection & Confidentiality Policy forms during induction and training of new team members and any in-house training in association with projects, particularly regarding holding or processing personal data at home.
7. Expressly include data protection activities in the FWinc Code of Conduct.
8. Include data protection in the FWinc Project Management Guidelines.
9. Include DPIAs in project and activity risk assessment templates and assessments.
10. Include procedures associated with data protection and confidentiality in project evaluation reports.
11. Be transparent with how we collect, use and store data by providing information on FWinc forms and the FWinc website.
12. Minimise the personal data requested and held.
13. Regularly clean data held and ensure it is up-to-date.
14. Reduce the amount of data sharing or copies of personal data to minimize the risk of security breaches.
15. Implement security measures including: using, where appropriate, artificial identifiers to replace identifying fields of any sensitive information; taking a register at activities where personal data forms in project folders are present.
16. Record consents on the FWinc electronic database including the following: how and when consent was obtained and by whom; which consents were or were not given and what information was provided to the data subject.
17. Record high-risk data processing activities (see below).
18. Record SARs and deletion requests and actions.
19. Record security measures in place.
20. Record steps taken to comply with the GDPR.
21. Record steps taken to ensure associate organisations and service providers are GDPR compliant (see section 18.2).
22. Record a data timeline (data mapping) to demonstrate the journey of personal data through the organisation.
23. Destroy hard-copies of personal data when no longer needed, by burning or shredding.
24. Review the FWinc Data Protection & Confidentiality Policy annually or as and when issues arise.
25. Review security features and measures annually.

18.1 Recording High-Risk Data Processing Activities

High-risk data processing activities are listed in Appendix D. High-risk data which FWinc is likely to process includes: criminal convictions during recruitment (Enhanced DBS checks); medical information (including mental health problems), bank account information, and name-address-date of birth.

If FWinc handles any high-risk data, the following information should be recorded:

- name and details of the organisation (and where applicable, of other controllers, your representative and data protection officer)
- relevant information of the data subject
- purposes of the processing
- description of the categories of individuals and categories of personal data
- retention schedules
- description of technical and organisational security measures.

18.2 External Organisations and Service Providers

To operate successfully, FWinc uses services provided by other organisations which, consequently, may have access to personal data. These include:

- Google (email provider – googlemail)
- Microsoft Windows (computer operating system and document software)
- HMRC
- Companies House
- Co-operative Bank (FWinc bank)

- Paypal (payment/donation method)
- Wix (website provider)
- MM&B (website domain name host)
- Heart Internet (website domain name server host)
- Facebook (social media)
- Twitter (social media)
- Youtube (social media)
- Accountants (if an audit is required)
- Funding Bodies and Organisations

FWinc should do its due-diligence to ensure these organisations are GDPR compliant. This involves: researching whether the organisations have released statements confirming their compliance; if not, contacting the organisations to confirm their compliance; enquiring where their data is stored, backed-up and whether in an country confirmed by the ICO as having adequate data protection law; and recording these steps as proof.

19. Implementation of this Policy

All adults in a supervisory or supporting role within FWinc will be made aware of this Policy, the content of this Policy and the schemes and procedures outlined within it upon training and induction into the organisation.

The actions outlined in Section 18 should be taken and a record of taking these actions and processing of high-risk data should be kept.

This Policy will be available at permanent premises used by FWinc and on the FWinc website.

20. Responsibilities

It is the responsibility of the FWinc Board of Directors to: appoint a FWincDL who is respected and informed and one whose duties, if already a FWinc team member, are compatible with the duties of the DC and would not lead to a conflict of interest; receive reports directly from the FWincDL as and when necessary; allow the DC to operate independently and not under threat of dismissal or penalisation for performing their task; ensure the FWincDL has adequate resources to meet their legal obligations; review this Policy and FWinc's security measures and DP ROPA annually or as and when issues arise.

It is the responsibility of the FWincDL to: inform and advise the organisation about their obligations to comply with the GDPR and other relevant legislation; inform the FWinc team and those who handle confidential information on best practice; maintain the FWinc DP Guidance document; advise on DPIAs; monitor compliance with the GDPR and other relevant legislation; ensure all confidential information is collected, used and stored in accordance with this Policy; liaise with associate organisations to ensure their compliance; maintain the FWinc electronic database; manage in-house procedures and any necessary disclosures of confidential information; ensure appropriate Privacy Statements and requests for consent are present on all FWinc forms used to obtain personal data; ensure a reference privacy statement is available on the FWinc website; maintain a record of consents given and withdrawn; maintain the record of data processing activities (ROPA) and actions taken to comply with the GDPR; be the point of contact for supervisory authorities and for data subjects; review and maintain security measures.

It is the responsibility of the FWinc Financial Director to: ensure the bank FWinc choose to use has sufficient data security measures in place to maintain privacy of FWinc workers and associates bank account details; to ensure any computer or device used for online banking has appropriate anti-virus and firewalls in place to maintain the security of any data held.

It is the responsibility of those inducting new team members to make them aware of this Policy and outline necessary procedures and provide them with guidance.

It is the responsibility of the FWinc team and all members and associates, should they be in possession of confidential information, to uphold this Policy and to follow any guidance provided to them.

21. Complaints

Complaints regarding the procedures or handling of the procedures mentioned in this Policy, the Policy itself or any other matter should follow the FWinc Complaints Procedure outlined in the FWinc Complaints Policy.

22. Review

This Policy will be reviewed by the FWinc Board of Directors annually or as-and-when issues arise or following updates so to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

GDPR-compliance, security measures and the DP ROPA should be reviewed annually by the FWinc Board of Directors.

23. External Contacts

Information Commissioner's Office (ICO): http://www.ico.gov.uk 0303 123 1113 (office hours)

Guidance: https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

24. Policy History

First version (Data Protection) adopted June 2009
Re-adoption July 2010 postponed for combining with the Confidentiality Policy
Second version (combined) adopted Feb 2011
Re-formatted May 2011
Amended and re-adopted Feb 2012
Re-adopted Feb 2013
Re-adopted March 2014
Re-adopted Feb 2015
Re-adopted June 2016
Re-adopted Jan 2017
Amended Nov 2017-Mar 2018
Re-adopted Mar 2018
Re-adopted Jan 2019
Re-adopted Jan 2020

Appendix A – Principles of Data Protection (DPA)

Fair and Lawful

Personal data should be processed fairly and lawfully. Organisations processing personal data need to be able to satisfy one or more 'conditions for processing'.

To be fair, organisations must: have legitimate grounds for collecting and using the personal data; be transparent—clear and open with individuals about how their information will be used; be honest about their identity; not use the data in ways that have unjustified adverse effects on the individuals concerned; give individuals appropriate privacy notices when collecting their personal data; handle people's personal data only in ways they would reasonably expect; not use an individual's personal data for a new purpose without their knowledge and/or consent; and make sure they do not do anything unlawful with the data.

'Lawful' refers to statute and to common law, whether criminal or civil. An unlawful act may be committed by a public or private-sector organisation.

Transparency is always important, but especially so in situations where individuals have a choice about whether they wish to enter into a relationship with organisations. If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

A decision to share personal data with another organisation does not take away an organisation's duty to treat individuals fairly. Before sharing personal data, organisations should consider carefully what the recipient will do with it and what the effect on individuals is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract. In some circumstances, disclosure to another organisation may be justified in the individual's best interests, but where none of the statutory exemptions apply.

Personal data should also be processed fairly, although this is not defined in the DPA. Information should be given to the individual by either actively communicating it or making it readily available. Preferably, this should occur in a statement, oral or written, when the personal data is collected. Such a notice should state at least the organisation's identity (and base in the UK) and the purpose for which they intend to process the information.

Processing may also be unlawful if it results in:

- a breach of a duty of confidence
- an organisation exceeding its legal powers or exercising those powers improperly
- an infringement of copyright
- a breach of an enforceable contractual agreement
- a breach of industry-specific legislation or regulations
- a breach of the Human Rights Act 1998, which, among other things, gives individuals the right to respect for private and family life, home and correspondence.

Purposes

Personal data should be obtained and held only for one or more specified and lawful purposes and should not be further processed in any manner incompatible with that purpose or those purposes.

This requirement aims to ensure that organisations are open about their reasons for obtaining personal data and that what they do with the information is in line with the reasonable expectations of the individuals concerned. Organisations must:

- be clear from the outset about why they are collecting personal data and what they intend to do with it
- comply with the Act's fair processing requirements including the duty to give privacy notices to individuals when collecting their personal data
- comply with what the Act says about notifying the Information Commissioner

- if they wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, ensure the new use or disclosure is fair

Organisations can specify the relevant purposes in a privacy notice given to individuals at the time their personal data is collected or in a notification given to the Information Commissioner. Personal data must not be processed for any purpose that is incompatible with the original purpose or purposes. To use or disclose personal data for a purpose that is additional to, or different from, the purpose for which it was originally obtained, organisations should get prior consent.

Adequacy

Organisations should only collect the personal data that is needed for the purposes specified and that it is sufficient for the purpose for which it was collected—adequate, relevant and not excessive.

To assess whether organisations are holding the right amount of personal data, they must first be clear about why they are holding and using it. They should take into account that this may differ from one individual to another. The personal data should not include irrelevant details and where sensitive personal data is concerned, it is particularly important to make sure organisations collect or retain only the minimum amount of information needed.

Accuracy

Organisations are obliged to ensure the accuracy of the personal data they process (correct and not misleading) and, where necessary, that it is kept up to date. Although, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. Organisations should take reasonable steps to: ensure the accuracy of any personal data they obtain; ensure that the source of any personal data is clear; carefully consider any challenges to the accuracy of information; and consider whether it is necessary to update the information.

Organisations will not be considered to have breached the fourth data protection principle as long as: they have accurately recorded information provided by the individual concerned, or by another individual or organisation; they have taken reasonable steps in the circumstances to ensure the accuracy of the information; and if the individual has challenged the accuracy of the information, this is clear to those accessing it. If organisations use the data in making decisions that may significantly affect the individual concerned or others, they must put effort into ensuring its accuracy including obtaining independent confirmation that the data is accurate. In circumstances where inaccurate information could have serious consequences, organisations should double-check it is correct. If individuals challenge the accuracy of the data held on them, and can provide convincing documentary evidence, organisations should delete or correct them. If an individual is not satisfied that organisations have taken appropriate action to keep their personal data accurate, they may apply to the court for an order that they rectify, block, erase or destroy the inaccurate information.

An expression of an opinion about an individual is classed as their personal data. An area of particular sensitivity is medical opinion. If a court is satisfied that an organisation is holding inaccurate personal data containing an expression of opinion that appears to the court to be based on that inaccurate data, it can order them to delete all of that data, including the expression of opinion.

Retention

Organisations are required to retain personal data no longer than is necessary for the purpose which it is obtained. Organisations should: review the length of time they keep personal data; consider the purpose or purposes for which they hold the information in deciding whether (and for how long) to retain it; securely delete information that is no longer needed for this purpose or these purposes; and update, archive or securely delete information if it goes out of date. Keeping information for extended periods of time increases the risk it will become inaccurate and the number of SARs an organisation may receive.

Organisations should regularly review the personal data they hold and delete anything no longer needed. Information that does not need to be accessed regularly, but which still needs to be retained, should be safely archived or put offline. Organisations must still ensure the data is held securely.

It is good practice to establish standard retention periods for different categories of information. Organisations should also take account of any professional rules or regulatory requirements or industry

practices that apply. It is also advisable to have a system to keep to the retention periods and for documenting and reviewing the retention policy.

Retention periods should be judged on: the current and future value of the information; the costs, risks and liabilities associated with retaining the information; and the ease or difficulty of making sure it remains accurate and up to date. Personal data should not be kept indefinitely "just in case", or if there is only a small possibility that it will be used although there may be good grounds for keeping keeping personal data for historical, statistical or research purposes.

Processing/Rights

An individual has: a right of access to a copy of the information comprised in their personal data; a right to object to processing that is likely to cause or is causing damage or distress; a right to prevent processing for direct marketing; a right to object to decisions being taken by automated means; a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed; and a right to claim compensation for damages caused by a breach of the Act. See Appendix B for information on rights.

Security

Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Not all security breaches have grave consequences: many cause embarrassment or inconvenience to the individuals concerned; individuals are entitled to be protected from this kind of harm as well.

Organisations should have appropriate security to prevent the personal data held being accidentally or deliberately compromised. Ignorance of risks and security measures is not an excuse. In particular, organisations should: design and organise security to fit the nature of the personal data held and the harm that may result from a security breach; be clear about who is responsible for ensuring information security; make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and be ready to respond to any breach of security swiftly and effectively.

Security measures should ensure that: only authorised people can access, alter, disclose or destroy personal data; those people only act within the scope of their authority; and if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned. The level of security should reflect the the nature of the information in question and the harm that might result from its improper use, or from its accidental loss or destruction. Assessments of appropriate measures should be regularly reviewed as technology advances and should consider the costs involved.

Transfer

Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (i.e. the other seven principles are upheld). An up-to-date list of countries which have an adequate level can be found at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

To assess adequacy, organisations should consider: the nature of the personal data being transferred; the country or territory of origin of the information in question; the country or territory of final destination of that information; how the data will be used and for how long; and the security measures to be taken in respect of the personal data in the country or territory where the data will be received.

Appendix B – Rights of the Individual (GDPR)

Right to be Informed

Individuals have the right to know what data is held on them, why the data is being processed and whether it will be given to any third party. Organisations have an obligation to provide 'fair processing information', typically through a privacy notice, over how they use personal data at the time of receiving the data. As of 25th May 2018, the information supplied about the processing of personal data must be: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

Right to Access

In order to verify the lawfulness of the processing, individuals have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information. They have the right to be given this information in a permanent form (hard copy) by a subject access request (SAR). As of 25th May 2018, this must be given within one month (reduced by 10 days) and free of charge; although, a 'reasonable fee', based on administrative costs, can be charged if a request is manifestly unfounded or excessive, particularly if it is repetitive, or for copies of the same information.

The period of compliance can be extended by a further two months where requests are complex or numerous. The individual must be informed within one month why the extension is necessary. You can refuse to respond to a request but you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Where possible, organisations should provide remote access to a secure self-service system which would provide the individual with direct access to their information.

Right to Rectification

Individuals have the right to have their personal data rectified if it is inaccurate or incomplete. If disclosed to third parties, where possible, organisations must inform them of the rectification. When a rectification is requested, organisations must respond within one month, extended by two months where the request for rectification is complex. If refused, organisations must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to Erasure or to be Forgotten

Individuals can request the deletion or removal of their personal data in specific circumstances: the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; if the individual withdraws consent; if the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; the personal data was unlawfully processed; in order to comply with a legal obligation; in relation to the offer of information society services to a child. As of 25th May 2018, the right to erasure is no longer limited to processing that causes unwarranted and substantial damage or distress.

Personal data collected of a person under the age of 18yrs, once 18, has the 'right to be forgotten' and can request for their data to be erased.

Refusal is acceptable for the following reasons: to exercise the right of freedom of expression and information; to comply with a legal obligation (e.g. financial, medical, safeguarding), for the performance of a public interest task or exercise of official authority; for public health purposes in the public interest; archiving purposes in the public interest; scientific or historical research; statistical purposes; or the exercise or defence of legal claims. If personal data has been disclosed to third parties, organisations must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Right to Restrict Processing

Individuals have a right to 'block' or suppress processing of personal data when: an individual contests the accuracy of the personal data; an individual has objected to the processing and you are considering whether your organisation's legitimate grounds override those of the individual; when processing is

unlawful, the individual opposes erasure and requests restriction instead; if organisations no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim. If personal data has been disclosed to third parties, organisations must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

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.

Right to Data Portability

Individuals can obtain and reuse their personal data for their own purposes across different services without hindrance to usability. This only applies to personal data an individual has provided, where the processing is based on the individual's consent or for the performance of a contract; or when processing is carried out by automated means. Organisations must provide the personal data in a structured, commonly used and machine readable form (structured so that software can extract specific elements of the data).

Organisations have one month, if requested by an individual, to transmit the data directly to another organisation if this is technically feasible. This can be extended by two months where the request is complex or you receive a number of requests but organisations must inform the individual within one month of the receipt of the request and explain why the extension is necessary. If organisations refuse a request, them must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Right to Object

Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); or processing for purposes of scientific/historical research and statistics. Organisations must offer a way for individuals to object online.

Individuals must have an objection on grounds relating to their particular situation. Organisations must stop processing the personal data unless: they can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

Regarding personal data for direct marketing purposes, organisations must stop processing as soon as an objection is received. There are no exemptions or grounds to refuse. Organisations must deal with an objection to processing for direct marketing at any time and free of charge. Regarding personal data for research purposes, individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing. If organisations are conducting research where the processing of personal data is necessary for the performance of a public interest task, they are not required to comply with an objection to the processing.

Organisations must inform individuals of their right to object at the point of first communication and in any privacy notices. This must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

Rights Related to Automated Decision Making and Profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Individuals have the right not to be subject to a decision when it is based on automated processing or it produces a legal effect or a similarly significant effect on the individual. Organisations must ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it. The right does not apply if the decision is: necessary for entering into or performance of a contract between you and the individual; is authorised by law; based on explicit consent; or when a decision does not have a legal or similarly significant effect on someone.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their: performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements. When processing personal data for profiling purposes, organisations must ensure that appropriate safeguards are in place.

They must: ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences; use appropriate mathematical or statistical procedures for the profiling; implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects. Automated decisions **must not** concern a child or be based on the processing of special categories of data unless you have the explicit consent of the individual or the processing is necessary for reasons of substantial public interest.

Appendix C – Other changes to the DPA 1998 (GDPR)

Consent
As of 25th May 2018, consent for holding data must be: freely given by someone over the age of 16 to a named organisation via a positive, opt-in method (i.e. not pre-ticked boxes, by inactivity or by default); specific; easily withdrawn; clearly requested; and kept separate from other terms and conditions. Organisations must verify that any person giving consent on behalf of a child is allowed to do so—is a parent or guardian. There must be granular options to consent to independent processing operations or passing on data to third parties. If existing consents and consent mechanisms do not meet the new GDPR standard, fresh consents must be obtained. There is no set time limit for consent once obtained properly. Its duration depends upon the context but should be reviewed and refreshed as appropriate.

Privacy by Design
As of 25th May 2018, privacy by design is an express legal requirement. Organisations have a general obligation to implement technical and organisational measures to consider and integrate data protection into processing activities and demonstrate data protection is a cornerstone of their business policy and practices.

Controllers
As of 25th May 2018, controllers are responsible for compliance with the principle of accountability and must be able to demonstrate such. They must ensure they have contracts with processors and that the contracts comply with the GDPR.

Processors
As of 25th May 2018, processors must record processing activities. Organisations with more than 250 employees must maintain thorough internal records of processing activities. Those with less than 250 employees must maintain records of high-risk processing activities.

Data Protection Officers
As of 25th May 2018, it a requirement that organisations appoint a Data Protection Officer (DPO) only in some circumstances; those being if an organisation: is a public authority; carries out large scale systematic monitoring of individuals; or carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

Security
Security requirements of the DPA are not changed under the GDPR. As of 25th May 2018, Organisations are still required to process personal data in a manner that ensures its security and protection against unauthorised or unlawful processing or accidental loss, destruction or damage. Organisations can use discretion to make decisions on their level of security: the standard vs cost of security measures and the impact vs likelihood of breaches should be considered. Decisions and security measures should be recorded in the ROPA.

Data Breaches
As of 25th May 2018, organisations have a duty to report data breach to the ICO within 72 hours where it is likely to result in a risk to the rights and freedoms of the individuals and/or have a significant detrimental effect on individuals such as resulting in: discrimination, damage to reputation, identity theft, financial loss, loss of confidentiality or any other significant economic or social disadvantage. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also notify directly those individuals concerned. Failing to notify a breach, when required to do so, could result in a significant fine up to €10 million or 2% of an organisation's global turnover.

Transfer
As of 25th May 2018, there are restrictions on the transfer of personal data outside the European Union, to third countries or international organisations in order to not undermine the new protections afforded to the individual.

Appendix D - FWinc Privacy Statement Template

First page to be kept by the data subject, second included in information form.

Request for Consent

We are required by the Data Protection Act 1998 to obtain your informed consent to hold your up-to-date personal data on our database [OR the up-to-date personal data of the above named child on our database]. Funny Wonders Inc. (FWinc) request permission to collect, hold and use your personal data [OR personal data of the above named child]. Please read the following Privacy Statement and then complete the form below.

FWinc Privacy Statement

Lawful Basis: FWinc collects personal data lawfully through consent obtained from the data subject. You are not obliged to provide the data requested in this form. Failing to provide the data will have no detrimental affect on your participation in our activities. OR For reasons of safety, FWinc require you to provide the information requested or answer the questions asked above.

Data Use: FWinc would like to collect your data for internal administration purposes and so that we are able to contact you about present and future Funny Wonders activities and/or news. We will contact you primarily via email or by text if preferred. To no longer receive such communication, please email us a request to unsubscribe from our mailing lists.

Data Processing: FWinc would like to use information such as age and location in statistical analysis for evaluation of our activities to help shape our future activities. Your personal data will not be used in any automatic decision making or profiling processes.

Data Sharing: FWinc recognises the expectation of the confidentiality of personal data. FWinc will not pass on your personal data to any third party unless it is publicly available or disclosure is lawfully required as outlined in the FWinc Data Protection & Confidentiality Policy. If any organisation is interested in you or any of your personal data, we will contact you with the request and pass to you their contact details. ***For FWinc team members: FWinc requires communication between team members. For this reason, email addresses and phone numbers may be shared to facilitate this.

Data Storage: FWinc will store your data in hard-copy and on the FWinc electronic database. Hard-copies and electronic devices will be stored in safe and secure environments. All electronic devices will be password-protected with appropriate firewalls and anti-virus software to prevent hacking or theft. The storage of your data will be managed by the FWinc Data Controller and held in accordance with the Data Protection Act 1998.

Duration of Storage: FWinc will retain your personal data for a maximum of twenty years. This is so that we can let you know about any future activities with which you may like to get involved, including anniversary celebrations.

Data Requests: you are entitled, at any time, to request to know what of your own personal data we hold. To make a Subject Access Request, please contact the organisation via email (hello@funnywonders.org.uk) detailing what information you would like to know.

Data Deletion: you are entitled, at any time, to withdraw your consent for us to hold your personal data. To request its deletion, please contact the organisation via email (hello@funnywonders.org.uk) detailing what information you would like us to delete.

Objections: you reserve the right to object to FWinc collecting, holding or using your personal data.

Complaints: if you consider FWinc to collect, hold or use your personal data unlawfully, you are entitled to complain to a supervisory authority.

Consents

By providing any personal data on the following forms, your consent for FWinc to collect your personal data is implied. Do not complete the forms if you do not consent to this.

Do you consent to FWinc holding your personal data for the duration of the project/activity in which you are participating?	YES ☐	NO ☐
Do you consent to FWinc contacting you about its present activities and those in which you are participating?	YES ☐	NO ☐
Do you consent to FWinc contacting you about its future activities? If no, your data will be erased at the end of the calendar year of the last contact regarding the project/activity in which you are participating.	YES ☐	NO ☐
If yes, do you consent to FWinc holding your personal data for up to five years after your last involvement/contact in order to contact you about its future activities?	YES ☐	NO ☐
If yes, do you consent to FWinc holding your personal data for up to twenty years after your last involvement/contact in order to contact you about its future celebrations, anniversaries or activities?	YES ☐	NO ☐
Do you consent to FWinc contacting you about similarly creative activities in our local area in which you may be interested and which FWinc may be involved with or helping to promote?	YES ☐	NO ☐
Do you consent to FWinc contacting you via: Email	YES ☐	NO ☐
Phone	YES ☐	NO ☐
Social Media	YES ☐	NO ☐
Letter	YES ☐	NO ☐
***For FWinc Team: Do you consent to FWinc sharing your email address and phone number with members of the FWinc Team to aid communication and delivery of FWinc activities?	YES ☐	NO ☐
***For FWinc Board: Do you consent to FWinc holding your personal data and inviting you to Board of Director meetings?	YES ☐	NO ☐

Acknowledgements

FWinc aims to comply with legislation regarding data protection. Do you acknowledge we have provided comprehensive information regarding how we will use and store your personal data?	YES ☐	NO ☐
FWinc aims to keep accurate and up-to-date records. Do you acknowledge that we hope you will keep us informed by of any changes to your personal data?	YES ☐	NO ☐

Sign: Date:

Appendix E – Data Processing Information (GDPR)

High-Risk Data Processing Activities

- those which could result in a risk to the rights and freedoms of individual
- processing special categories of data (see below)
- processing criminal convictions and offences
- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals
- processing considerable amounts of personal data of a large number of individuals
- large scale, systematic monitoring of public areas

Conditions of Processing

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

Permitted Processing of Special Categories of Data

- the individual whom the sensitive personal data is about has given explicit consent to the processing.
- necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- in relation to personal data manifestly made public by the data subject
- necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.