

|  |
| --- |
| **THE RUISLIP-NORTHWOOD FESTIVAL ASSOCIATION** |
| **GENERAL DATA PROTECTION REGULATION 2018** |
| **DATA PROTECTION POLICY** |
|  |
| **Chris Lee** |
| **18th May 2018** |
| **Ver 1.2** |

# The Ruislip-Northwood Festival Association

# Data Protection policy

# Introduction

# The Ruislip-Northwood Festival Association is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

# We hold personal data about Teachers, Parents, Individuals and Competitors for the sole purpose of organising and running the Ruislip-Northwood Festival.

This policy sets out how we seek to protect personal data and ensure that the committee understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires the Ruislip-Northwood Festival Association committee be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

# Definitions

|  |  |
| --- | --- |
| **Business purposes** | The purposes for which personal data may be used by us:  *Business purposes include the following:*  Organising the annual Ruislip-Northwood Festival for Dance, Music and Speech & Drama.  Compiling the Timetable of classes at each of our three sections.  Compiling a programme of all competitors taking part in each section.  Providing Report Sheets and Certificates for competitors  Recording and publishing results of all medal winners. |

|  |  |
| --- | --- |
| **Personal data** | Personal data’ means 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. *Personal data we gather may include: individuals' name, address, phone number, email address, Competitors Age/Date of Birth (so that we can allocate them to the correct age class)* |
| **Special categories of personal data** | Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information.**.** |
| **Data controller** | ‘Data 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 law. |
| **Data processor** | ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| **Processing** | ‘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. |
| **Supervisory authority** | This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office. [www.ico.org.uk](http://www.ico.org.uk). |

# Scope

This policy applies to all Ruislip-Northwood Festival Association committee members, who must be familiar with this policy and comply with its terms.

This policy supplements any other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to the committee before being adopted.

Who is responsible for this policy?

As our Chairman, Mr. Christopher Lee has overall responsibility for the day-to-day implementation of this policy. You should contact him for further information about this policy if necessary.

Mr. Christopher Lee.

Chairman,

Ruislip-Northwood Festival Association,

1, Midcroft.

Ruislip.

Middlesex.

HA4 8ET

# The principles

The Ruislip-Northwood Festival Association shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

**1. Lawful, fair and transparent**

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

**2. Limited for its purpose**

Data can only be collected for a specific purpose.

**3. Data minimisation**

Any data collected must be necessary and not excessive for its purpose.

**4. Accurate**

The data we hold must be accurate and kept up to date.

**5. Retention**

We cannot store data longer than necessary.

**6. Integrity and confidentiality**

The data we hold must be kept safe and secure.

Accountability and transparency

The Ruislip-Northwood Festival Association must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. We are responsible for keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the Festival Committee.

To comply with data protection laws and the accountability and transparency Principle of GDPR, The Ruislip-Northwood Festival Association must demonstrate compliance. We are responsible for understanding our particular responsibilities to ensure we meet the following data protection obligations:

* Fully implement all appropriate technical and organisational measures
* Maintain up to date and relevant documentation on all processing activities
* Conducting Data Protection Impact Assessments
* Implement measures to ensure privacy by design and default, including:
  + Data minimisation
  + Pseudonymisation
  + Transparency
  + Allowing individuals to monitor processing
  + Creating and improving security and enhanced privacy procedures on an ongoing basis

# Our procedures

Fair and lawful processing

The Ruislip-Northwood Festival Association must process personal data fairly and lawfully in accordance with individuals’ rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs. processing data

The Ruislip-Northwood Festival Association is classified as a [data controller and data processor].

Section Secretaries: As a data processor, we must comply with our obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

* Not use a sub-processor without written authorisation of the data controller
* Co-operate fully with the ICO or other supervisory authority
* Ensure the security of the processing
* Keep accurate records of processing activities
* Notify the controller of any personal data breaches

If in any doubt about how we handle data, contact the Festival Chairman for clarification.

Lawful basis for processing data

The Ruislip-Northwood Festival Association must establish a lawful basis for processing data. Ensure that any data we are responsible for managing has a written lawful basis approved by the Festival Committee. It is our responsibility to check the lawful basis for any data we are working with and ensure all of our actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual’s data to be processed for a specific purpose.

1. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

1. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

1. **Vital interests**

Processing the data is necessary to protect a person’s life or in a medical situation.

1. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

1. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.

Deciding which condition to rely on

Consider the following factors and document answers:

* What is the purpose for processing the data?
* Can it reasonably be done in a different way?
* Is there a choice as to whether or not to process the data?
* Who does the processing benefit?
* After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
* What is the impact of the processing on the individual?
* Are you in a position of power over them?
* Are they a vulnerable person?
* Would they be likely to object to the processing?
* Are you able to stop the processing at any time on request,

and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

The Ruislip-Northwood Festival Association are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, this must be approved by the Festival Committee.

# Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person’s fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual’s:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sexual orientation

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

# Responsibilities

The Ruislip-Northwood Festival Association responsibilities

* Analysing and documenting the type of personal data we hold,
* Checking procedures to ensure they cover all the rights of the individual,
* Identify the lawful basis for processing data
* Ensuring consent procedures are lawful,
* Implementing and reviewing procedures to detect, report and investigate personal data breaches,
* Store data in safe and secure ways,

Assess the risk that could be posed to individual rights and freedoms should data be compromised:

* Fully understand our data protection obligations,
* Check that any data processing activities we are dealing with comply with our policy and are justified,
* Do not use data in any unlawful way,
* Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions,
* Comply with this policy at all times,
* Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay,

Responsibilities of the Festival Committee

* Keeping Festival members and volunteers updated about data protection responsibilities, risks and issues,
* Reviewing all data protection procedures and policies on a regular basis,
* Arranging data protection training and advice for all committee members and those included in this policy,
* Answering questions on data protection from committee members and volunteers,
* Responding to individuals such Teachers, Parents and competitors (over 16 years of age) who wish to know which data is being held on them by us,
* Checking and approving with third parties that handle the Ruislip-Northwood Festivals data any contracts or agreement regarding data processing,

Responsibilities of Section Sectretaries

* Ensure all systems, services, software and equipment meet acceptable security standards,
* Checking and scanning security hardware and software regularly to ensure it is functioning properly,
* Researching third-party services, such as cloud services the company is considering using to store or process data,
* Approving data protection statements attached to emails and other marketing copy,
* Addressing data protection queries from clients, target audiences or media outlets,
* Coordinating with the Festival Committee to ensure all marketing initiatives adhere to data protection laws and the Festival’s Data Protection Policy,

Accuracy and relevance

The Ruislip-Northwood Festival Association will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Festival chairman or relevant Section Secretary.

Data security

Section Secretaries must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Festival Committee will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

* In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
* Printed data should be shredded when it is no longer needed.
* Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all Committee members to use a [password manager](http://cybersecurityzen.com/cybersecurity/keep-data-safe-rise-password-managers-1654/) to create and store their passwords.
* Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
* The Festival Committee must approve any cloud used to store data.
* Servers containing personal data must be kept in a secure location.
* Data should be regularly backed up in line with the Ruislip-Northwood Festival Association backup procedures.
* Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
* All servers containing sensitive data must be approved and protected by security software.
* All possible technical measures must be put in place to keep data secure.

Data retention

* The Ruislip-Northwood Festival must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

The Ruislip-Northwood Festival Association do not transfer personal data outside of the United Kingdom.

# .

# Rights of individuals

Individuals have rights to their data which the Ruislip-Northwood Festival must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

**1. Right to be informed**

* Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
* Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

**2. Right of access**

* Enabling individuals to access their personal data and supplementary information.
* Allowing individuals to be aware of and verify the lawfulness of the processing activities.

**3. Right to rectification**

* We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
* This must be done without delay and no later than one month. This can be extended to two months with permission from the Festival committee.

**4. Right to erasure**

* We must delete or remove an individual’s data if requested and there is no compelling reason for its continued processing.

**5. Right to restrict processing**

* We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
* We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

**6. Right to data portability**

* We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
* We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

**7. Right to object**

* We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
* We must respect the right of an individual to object to direct marketing, including profiling.
* We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

**8. Rights in relation to automated decision making and profiling**

* We must respect the rights of individuals in relation to automated decision making and profiling.
* Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

# Privacy notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

* Identification and contact information of the data controller and the data protection officer
* The purpose of processing the data and the lawful basis for doing so
* The legitimate interests of the controller or third party, if applicable
* The right to withdraw consent at any time, if applicable
* The category of the personal data (only for data not obtained directly from the data subject)
* Any recipient or categories of recipients of the personal data
* Detailed information of any transfers to third countries and safeguards in place
* The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
* The right to lodge a complaint with the ICO, and internal complaint procedures
* The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
* Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
* Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

# Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How The Ruislip-Northwood Festival Association deal with subject access requests

The Ruislip-Northwood Festival Association must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt. The Festival endeavours to provide data subjects access to their information in commonly used electronic formats.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the Festival Committee before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the Festival Committee.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

The Ruislip-Northwood Festival Association must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the Festival Committee first.

# Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed,
* Where consent is withdrawn,
* Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing,
* The personal data was unlawfully processed or otherwise breached data protection laws,
* To comply with a legal obligation,
* The processing relates to a child,

How we deal with the right to erasure

The Ruislip-Northwood Festival Association can only refuse to comply with a right to erasure in the following circumstances:

* To exercise the right of freedom of expression and information
* To comply with a legal obligation for the performance of a public interest task or exercise of official authority
* For public health purposes in the public interest
* For archiving purposes in the public interest, scientific research, historical research or statistical purposes
* The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The Ruislip-Northwood Festival Association do not pass personal data to third parties with the exception of information required by All England Dance for qualifying competitors to be able to take part in the AED Regional Finals.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. The Ruislip-Northwood Festival Association must cease processing unless:

* We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
* The processing relates to the establishment, exercise or defence of legal claims.

The Ruislip-Northwood Festival Association must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

* It is necessary for the entry into or performance of a contract.
* Based on the individual’s explicit consent.
* Otherwise authorised by law.

In these circumstances, we must:

* Give individuals detailed information about the automated processing.
* Offer simple ways for them to request human intervention or challenge any decision about them.
* Carry out regular checks and user testing to ensure our systems are working as intended. The Ruislip-Northwood Festival do not carry out automated profiling or decision making.

# Third parties

Using third party controllers and processors

As a data controller and data processor, we must have written contracts in place with any third party [data controllers (and/or) data processors] that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

[For controllers] As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

[For processors] As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

The Ruislip-Northwood Festival Association contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with [data controllers (and/or) data processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

* Acting only on written instructions,
* Those involved in processing the data are subject to a duty of confidence,
* Appropriate measures will be taken to ensure the security of the processing,
* Sub-processors will only be engaged with the prior consent of the controller and under a written contract,
* The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR,
* The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments,
* Delete or return all personal data at the end of the contract,
* Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations,
* Nothing will be done by either the controller or processor to infringe on GDPR,

.

.

# Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The Ruislip-Northwood Festival Association must conduct a regular data audit as defined by the Festival Committee and normal procedures.

Monitoring

Everyone must observe this policy. The Festival Committee has overall responsibility for this policy. The Ruislip-Northwood Festival Association will keep this policy under review and amend or change it as required. We must notify the Festival Committee of any breaches of this policy. We must comply with this policy fully and at all times.

Training

Committee members will receive adequate training on provisions of data protection law specific for their role. Committee members must complete all training as requested. If they move role or responsibilities, and are responsible for requesting new data protection training relevant to their new role or responsibilities.

If Festival Committee require additional training on data protection matters, contact the FestivalChairman.

# Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. The Ruislip-Northwood Festival Association has a legal obligation to report any data breaches to the ICO] within [72 hours].

All Committee members have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a register of compliance failures,
* Notify the ICO ] of any compliance failures that are material either in their own right or as part of a pattern of failures,

Any Committee member who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to the RNF Chairman for our reporting procedure.

Failure to comply

The Ruislip-Northwood Festival take compliance with this policy very seriously. Failure to comply puts both committee members and the organisation at risk.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Festival Chairman.