National Youth Orchestra of Ireland
Ceolfhoireann Náisiúnta Óige na hÉireann

Transparency & GDPR
Data protection policies

Updated: October 2025
Next update due: October 2027

Contents

INTRODUCTION – OUR APPROACH TO DATA PROTECTION 3

HOW WE PROTECT YOUR DATA 3

Lawful 3

Fair 3

Clear 4

Accurate 5

Secure 5

Accountable 5

YOUR DATA AND YOUR RIGHTS 5

‘Access’ to your data 5

‘Rectification’ – the power to correct your data 5

‘Erasure’ – the power to have your data wiped from our records 5

‘Restriction’ – your right to challenge how we use your data 5

‘Portability’ – your right to reuse data in more than one organisation 6

‘Objection’ – your right to object to us using your data 6

‘Opt out’ – your power to opt out of automated decision-making 6

Right to complain 7

OUR RESPONSIBILITIES AS A ‘DATA CONTROLLER’ 7

Technical and organisational systems 7

Adequate record keeping about how we use data 7

Type of data we have on record 7

Data sharing with third parties 8

Data breach 8 Record keeping 8

Responsibilities of staff and others 8

Consequences of failing to comply 9

APPENDIX - OCTOBER 2025 UPDATE 10

International Transfers of Personal Data 10

Protecting Children’s Personal Data 10

Strengthening Data Breach and Security Measures 10

Introduction – our approach to data protection

The General Data Protection Regulation (GDPR) and the Irish Data Protection Legislation tells us and other organisations how we must handle data about people.

'Data' means any information about people we collect.

'Data processing' is a phrase used to describe all the different ways data is used and stored. This Data Protection Policy tells you how the National Youth Orchestra of Ireland (NYOI) handles and protects any data we gather about you to make sure that we comply with these laws.

We gather data about:

- employees and contract staff
- members and applicants for membership
- other individuals
- other suppliers

This means that we control data and we are a 'data controller'.

As well as using your data to facilitate our interaction with you, we use it in anonymised forms to contribute to our analysis of our work (the number of young people involved in our work, their age and instrumental specialisms, their geo location), and to be accountable to funders and other stakeholders in our work.

How we protect your data

Our policy covers all the data, including personal and sensitive details that we collect about people. It covers data held on paper and on computers. We will treat all data with equal care.

We take care to make sure we handle your data appropriately. To this end, we are lawful, fair and clear. This means:

Lawful

Generally, how we handle data is based on legislation under the General Data Protection Regulation (GDPR) Articles 6.1 (a), (b), (c), and (f). This means we will ask your permission to handle your data when necessary. You can withdraw your consent at any time.

However, to enter any contract with us, you must give us permission to handle your data. So, if you withdraw your consent to use any of your data, we must withdraw our services from you.

Fair

For data processing to be fair, we have to make certain data available to you. We will only handle data in ways that people would reasonably expect us to do so, and

we will not use your data in ways that might damage you unfairly.
We must do this if we got the data directly from you, or from other sources. You may have forgotten what information you gave us and wish to see what it was.

Clear
We will provide necessary data to you when you need it. When we provide data we make sure it is detailed and specific, clear and in plain language.

We make data available through our websites, forms and publications. We gather data only as needed to provide services.

We design systems to collect data so we can gather and use it only for the purpose for which we collect it, and so we can provide the services you have asked for. This applies to online forms, hard copy documents and other ways of collecting data.

Our employees must only accept a request for data from another organisation or person if it is directly related to the reason we collected the data in the first place. Even if the reason seems related, our staff must not reveal data unless it is why we originally collected your data.

If we need to give your data to another organisation or person we must first assess the impact this will have on you before sharing it and ensure the organisation also complies with GDPR. This assessment is called a 'Data Protection Impact Assessment' (DPIA).

We also take care to ensure the data we hold is accurate, secure and held in an accountable way. This means:

Accurate
We will make sure any data we keep about you is accurate and up to date. We need to do this so we can provide our services. You have the right to make sure the data we hold about you is accurate and complete.

We design the ways we collect data so that it is easy to update information when we get new data. If we have provided data about you to third parties which is no longer accurate, we will give them the updated data. However, we will not do this if it is impossible or requires significant time or effort to do so. For example, if you change your mobile number and we do not have any other contact data to reach you.

We will keep your data only for as long as needed. The legislation says we should keep any data that identifies you only for as long as we need it to provide our service to you. We put in place policies and procedures to make sure that we keep any data that identifies you for the least amount of time needed so we can operate effectively. We have systems in place to
destroy or remove data that identifies you after we no longer need it.

Secure
The law requires us to use technical and organisational security measures when handling data to protect against unauthorised or unlawful access as well as accidental loss, destruction or damage.

We have put in place the necessary measures to do this.

Accountable
We are accountable for, and able to show how we comply with the data protection legislation. We do this by using appropriate records and systems for handling your data.

Your data and your rights

We design and maintain appropriate policies, procedures and staff training to make sure we fulfil the legal rights related to your data.

'Access' to your data
Under the Right of Access by the data subject (GDPR, Article 15), you have the right to access any of your data which is being processed by us. We put in place ways of working that make sure when you ask for details of data we hold about you, we can find and provide the data. We do this within the time allowed in the legislation.

'Rectification' – the power to correct your data
Under the Right to Rectification (GDPR, Article 16) If you think we hold inaccurate or incomplete data about you, you have the right to ask us to correct it. We have systems in place to make sure that we can correct data about you that is inaccurate.

'Erasure' – the power to have your data wiped from our records
Under the Right to Erasure sometimes called the 'right to be forgotten' (GDPR, Article 17) You have the right to ask us to delete or remove your data where there is no reason for us to keep it. If this is possible we will do so.

In some cases, there may be some legal reason why we cannot remove your data. For example, where we must perform a task in the public interest, or keep your data because it is related to a legal claim, or keep your data for our archive.

'Restriction' – your right to challenge how we use your data
Under the Right to restriction of processing (GDPR, Article 18), if you ask us to limit how we use your data, we will do so if the following circumstances apply. You argue that:

- the data we hold about you is inaccurate
- the NYOI no longer needs the data, but you do
- you have already lodged an objection to the NYOI about using your data.

You may also argue that processing your data is unlawful. You may be against us wiping out

your data, but ask us to restrict its use instead. To do this, we will put in place and maintain appropriate procedures. They enable us to assess if your request to restrict the processing of your data can be put in place. We will write to you:

- confirming we received your request
- if we can carry out your request
- when we have carried out your request.

If we later decide to use your data again, we will first write to you to let you know.

'Portability' – your right to reuse data in more than one organisation

Under the Right to Data Portability (GDPR, Article 20), you have the right to get and reuse your data across different organisations. Where we collect your data with your consent or through a contract, you have a right to receive this data from us in electronic format. This allows you to move, copy or transfer data easily from one IT environment to another. It makes this safe and secure and your data easier to use. You can then give this data to a data controller in another organisation. We will put in place appropriate procedures so that we transfer only the relevant data.

'Objection' – your right to object to us using your data

Under the Right to Object (GDPR, Article 21), you can object to us using your data. We may still use it if we

- can show compelling reasons why we need to do so
- can show we need to use your data in the public interest
- need your data to defend legal claims.

However, we will stop using your data if you tell us you object to us doing so for

- direct marketing
- scientific research
- historical research
- statistical analysis.

If we need to use your data in the public interest for scientific or historical research or statistical analysis we will make sure that you cannot be identified. This is known as anonymisation.

'Opt out' – your power to opt out of automated decision-making

We don't use 'automated decision making' but if we ever do, we will ask you first under the Right to Opt Out of automated individual decision-making (GDPR, Article 22).

Sometimes when organisations hold data about you, they use an automated decision system to decide things about you. However, if this type of decision would have a legal or significant effect on you, you can tell the organisation not to do so. Currently we do not use any such automated decision making processes.

If we ever decide to use your data in this type of system in the future, we will tell you in

advance and give you the right to object.

Right to complain
If you wish to complain about how we use your data, you can contact our GDPR Compliance Officer. The GDPR Compliance Officer will work with you to resolve your complaint. If you are not satisfied with how we resolved your complaint, the Officer will tell you about your right to bring your complaint to the Data Protection Commission. They will also give you the appropriate contact details.

Our responsibilities as a 'Data controller'

The NYOI is considered a 'data controller'. A data controller is responsible for deciding how to use the data of its clients, staff and other stakeholders. Stakeholders are people with an interest in an organisation and or its work.

We are committed to complying with the data protection legislation.

Technical and organisational systems
We have technical and organisational systems to manage your data. We have designed these to make sure we can protect your data. We update these systems as needed. These systems also mean that we can clearly show how we use your data securely, as follows:

- We have put in place appropriate security standards to protect your data.
- Only those who have the appropriate authorisation may access your data.
- If there is ever an incident affecting our systems, we can restore the availability and access to data in a timely manner.
- We regularly test, assess and evaluate how effective our organisational and technical measures are.

Adequate record keeping about how we use data
We are required to keep appropriate records of processing activities under GDPR Article 30.

We will keep a record of how we use data as required by the legislation. We will review this at least once a year and make it available to the Data Protection Commission on request. If there are any significant changes to an existing process or if we put in place a new process, we will let the relevant manager know so they can update the records.

Type of data we have on record
We keep the name and contact details of the data controller and a relevant contact person.

We also keep a record of the types of business systems we use, categories of data we hold, and why it is legal for us to use data in the way that we do. We keep records of how long we can keep each type of data for, when and why we share data with another organisation, when we have transferred data to a third country (and what country that is), and the type of technical and organisational security measures we have put in place.

Our systems are designed to protect your data (Data protection by design and default, GDPR Article 25). When we are planning to introduce new systems or technologies, one of the first things we do is decide how to make sure we can continue to protect data.

Data sharing with third parties

We will not share your data with any other organisation unless there is a lawful reason for us to do so or to provide you with the service you have requested. We will seek your consent to share your information with another organisation.

Before we share any data with any other organisation, we put a written agreement in place. It includes how this data will be handled. By 'third party' we mean anyone or organisation, whether a part of the NYOI or outside the NYOI, who manages data on our behalf. The agreement states:

- Why data needs to be shared between us and a third party
- The right to terminate processing that we or the third party can take
- The third party may not transfer data to any other person or organisation
- If the third party is asked for data, they will provide it to us
- The right for us to audit the data that the third party holds.

Data breach

A 'data breach' is a gap in security that leads to the accidental or illegal destruction, loss, alteration, unauthorised disclosure of, or access to data.

If our security fails and there is a 'data breach' (for example when correspondence is sent to an unauthorised third party), the person responsible will notify the GDPR Compliance Officer. The General Manager along with the GDPR Compliance Officer will assess the severity of the breach.

Where appropriate they will notify the Data Protection Commission within 72 hours. Where a breach is likely to result in a high risk to the rights and freedoms of the people whose data has been compromised, we will notify them about the breach.

Record keeping

We keep logs of relevant data protection related events, for example:

- If you ask us for any of your legal rights to be respected (this is called 'invocation of subject rights')
- When data is used inappropriately
- When we carry out an assessment to see if we need to do a Data Protection Impact Assessment (DPIA).

Responsibilities of staff and others

Anyone who processes data on our behalf must comply with this data protection policy. All records created on our behalf belong to us.

Anyone who handles data we hold must read, understand and accept all our data protection policies, procedures and guidelines.

They must also make sure that when they access, manage and control data as part of

their daily duties, they do so in line with data protection requirements. Everyone who handles data on our behalf must also make sure they comply with our data protection rules.

Consequences of failing to comply

We take compliance with this policy very seriously. If we fail to comply, it puts individuals and the organisation at risk. Individuals who fail to follow our data protection policies may be subject to disciplinary procedures. If staff consider that this policy has not been followed, they should raise the matter through their manager or with the Board.

Appendix - October 2025 Update

International Transfers of Personal Data

If we transfer personal data outside the European Economic Area, we will make sure it remains properly protected. To do this, we will check that any organisation receiving the data follows data protection rules that offer the same level of protection as in Ireland and the EU. Where needed, we will use approved safeguards such as Standard Contractual Clauses and carry out assessments to confirm that the laws in other countries do not reduce the level of protection for your data. If we cannot guarantee your data is protected to the required standard, we will not transfer it.

Protecting Children's Personal Data

When collecting or handling data from children or young people, we will take extra care to ensure their rights and best interests are protected. This includes providing information in clear language, using high privacy settings by default, avoiding reliance on "legitimate interests" unless it clearly supports a child's rights, and asking for parental consent when required. If any of our services are likely to be used by children, we will complete assessments to identify and reduce risks before collecting their data.

Strengthening Data Breach and Security Measures

We will keep strong systems and controls in place to protect personal data and prevent breaches. If something does go wrong and personal data is exposed or lost, we have procedures to act quickly, assess the risk, and notify the Data Protection Commission and the individuals affected when the law requires it. We will regularly test our security processes to make sure they work effectively and keep up with legal obligations.