



Face Front Inclusive Theatre

52 Market Square, Edmonton Green, London N9 0TZ

Tel - 020 8350 3461 | Email - admin@facefront.org | www.facefront.org

Data Protection Policy

Face Front needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Face Front Inclusive Theatre:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulation 2018 describes how Face Front must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Inclusion Through Theatre

Patrons: Mat Fraser | Josette Bushell-Mingo OBE | Rachel Denning | Doris Jaggge
Aditya Chakrabortty | Onjali Rauf MBE | Joseph Adalakun | Jamie Beddard

Face Front Inclusive Theatre is a company limited by guarantee.
Registered in England and Wales No.05154096. Registered Charity No.1116506.

Policy scope

This policy applies to:

- The head office of Face Front
- All venues Face Front operates in
- All staff and volunteers of Face Front
- All contractors, suppliers and other people working on behalf of Face Front
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 1998.

What data we collect

We collect data information when individuals buy tickets for our performances, join one of our groups, join the Face Front team as a Trustee, Staff member, Freelancer or volunteer.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone number
- Country of residence
- Plus any other information relating to individuals

Data protection risks

This policy helps to protect Face Front from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Face Front has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Trustees** are ultimately responsible for ensuring that Face Front meets its legal obligations.

The CEO is the GDPR lead manager and is responsible for:

- Keeping the Trustees updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

Face Front's performing arts groups



- Dealing with requests from individuals to see the data Face Front holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Staff guidelines

The only people able to access data covered by this policy should be those who **need it for their work**.

- Data **must not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Face Front will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

Storing data safely is the responsibility of all Face Front employees and freelance staff.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

Face Front's performing arts groups



When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Security whilst working with Data

When personal data is accessed and used it is at the greatest risk of loss, corruption or theft. Therefore, when accessing data these guidelines should be observed:

When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.

- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data use

Personal data will be held on Face Front's system and used for mailing list subscriptions and to provide users with services, products or information they have requested.

We will not sell, trade, or rent personal information to others without permission and we will only use information in accordance with the individuals' decisions. Individuals can change their choices about how Face front uses personal information at any time, via our website or by contacting our Office at info@facefront.org.

We may analyse personal information from our website users and log files created to record the details of visits to our website. Log file information does not allow individuals to be personally identified.

We will always update those involved about how we will use any further information given to us.

Data accuracy

The law requires Face Front to take reasonable steps to ensure data is kept accurate and up to date.

Face Front's performing arts groups



The more important it is that the personal data is accurate, the greater the effort Face Front should put into ensuring its accuracy.

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Face Front will make it **easy for data subjects to update the information** Face Front holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the CEO's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access request

All individuals who are the subject of personal data held by Face Front are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the info@facefront.org

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Face Front will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Trustees and from the company's legal advisers where necessary.

Providing information

Face Front aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used

Face Front's performing arts groups



- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

A version of this statement is also available on the company's website.

Related Policies and procedures

This policy should be read alongside our related organisational policies:
Child and Vulnerable Adult Safeguarding policy

LAST REVIEWED

December 2025

REVIEW

June 2026

Face Front's performing arts groups

