GDPR

UK DATA PROTECTION ACT 2018 & EU GENERAL DATA PROTECTION REGULATION

The Data Protection Act and GDPR is no one's favourite subject, but it is important to acknowledge and act accordingly to ensure sensitive personal information is kept safe and secure to prevent anyone's data (particularly young people's) from being exposed to the wrong person. At StreetGames, we've taken time to compile what we think are the most useful top tips and 'need to knows' for Locally Trusted Organisations regarding data protection.

DATA COLLECTION

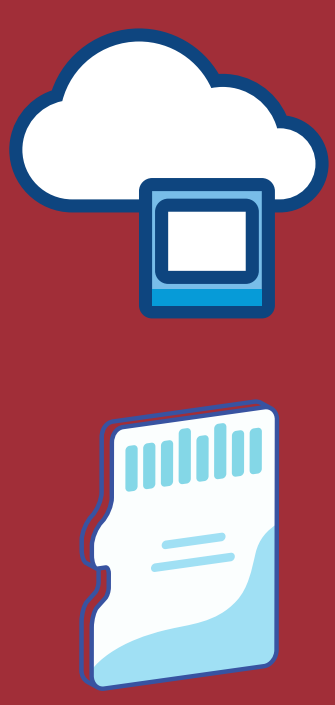
It should always be made clear to the person why their personal data is being requested, for instance if a participant asks – it is to show your stakeholders who is attending to show impact and secure future funding. It is good practice to have a statement or simplification of your privacy policy to hand to give to anyone who requests this.

Questions should be asked only on a need-to-know basis, with a clear purpose for using the information. For instance, demographic questions are often asked as it is important to gain a demographic profile of session participants to highlight future target audiences.

When asking certain information, parental consent may be needed for people aged under 16. It is good practice to have a consent form template to hand with clear points stating what you want to collect, why and exactly how it will be used.

DATA STORAGE

Be sure to make sure your smartphone or laptop is locked with a password/pincode and also has a short automatic lock setup, so that your device is secure when you walk away from it. If you ever store or download sensitive data on your device, it's best to also password protect these files if possible.



If you have sensitive data in physical form, such as paper registers, ensure these are locked away safely out of reach. When they are no longer needed or the data has been transferred onto a computer, it is best to dispose of them securely by shredding the paper versions.

In the event of personal data being lost or stolen, it is responsible to contact those who may be affected and if possible, provide support to the victims and set out a plan to mitigate any further breaches.

Personal data should only be held for the length of time relevant to its purpose, for example if a participant has not attended for a number of years their personal data is no longer needed.

DATA SHARING

Before sharing any personal data – check that you have permission and there is a valid reason for doing so. You may in some cases share information without consent if there is a lawful reason for doing so, such as where safety may be at risk.

Please be wary of including any sensitive personal data within the body of an email, as they can be easily intercepted and read in some circumstances.

If your email must contain sensitive data, make sure it as attached as a separate document and password protected. The password is then best shared with the recipient via another form of communication such as text or phone call.

There are lots of secure ways to share files nowadays, if your organisation uses a cloud service such as OneDrive or DropBox, you can share files and folders securely with access permitted only for specific people. You can use the same method via online sharing platforms too, such as WeTransfer.

Data Protection Act and GDPR is often easy to forget about when shouting about the great work we are doing, so be sure to reflect on the permissions you've been granted when disseminating things like reports and case studies. For example, check that you have photo consent from everyone pictured in a report and anyone who is identifiable by name, has given permission for their story to be shared in this way.

When disseminating, if you do not have permissions from the people involved to share their data, or the end user has no reason to know of the personal information it should then be anonymised so that those people are 'unidentifiable'.