GDPR and the Doorstep Data Protection Policy – an Introduction

GDPR came into place May 25 2018 and will affect ALL businesses including non-for-profit organisations such as ourselves…

What is GDPR? GDPR builds on the existing 1998 Data Protection Regulations and came into force on the 25th May 2018. Working with Doorstep Arts will require that you understand our policies in respect of GDPR and understand the importance of our being GDPR compliant and what you need to do to work with us.

How have our policies been created? Doorstep Arts as a company is very aware of the importance of Data Protection, in line with the 25 May GDPR regulations we have reviewed our existing policies and procedures and want to make sure that everyone who works with us understands the importance of GDPR, as an individual an for Doorstep as a whole. The policies are going to grow organically as we as a Company grow, ensuring best practice, so as always please make sure you talk to us if there is anything you do not understand, think can be improved on, or if you are concerned does not take into consideration a particular aspect of your job.

What are the data protection principles behind GDPR? There are 8 main principles, these are that personal information:

must be fairly and lawfully processed

must be processed for limited purposes

must be adequate, relevant and not excessive

must be accurate and up to date

must not be kept for longer than is necessary

must be processed in line with *data subjects' rights

must be secure

must not be transferred to other countries without adequate protection

for more info on data subjects' rights see:
https://www.scl.org/articles/3575-rights-of-data-subjects-under-the-gdpr

NON compliance could see business fined up to 20m euros or 4% or their global turnover – whilst it is unlikely that companies such as Doorstep Arts will be fined, and the ICO is there to support companies in making sure that they are compliant, non-compliance could cause huge reputational damage.

What is personal data? Personal data is any information relating to an identified or identifiable living person and includes:

Name
Contact details
Identification Number
Online identifier such as a username

More sensitive data includes:

Racial or ethnic origin
Political opinions
Religious beliefs
Trade union membership
Genetic information
Biometrics
Health – mental OR physical
Sex life & sexual orientation

What is data processing? This is anything that is done to personal data, including collecting, recording, organising, structuring, storing, retrieving, using, erasing or destroying

It is useful to data protection does apply to anonymised data or data that cannot be linked to a specific individual, but most importantly **REMEMBER** just like safeguarding and H & S it is **EVERYONE'S RESPONSIBILITY.**

Doorstep have put together a list of **Do's** and **Don'ts** which can be found on pages 7 and 8 and make up part of the **Doorstep Arts Data Protection Policy** , have a look and make sure you are doing everything you need to, anything you think has been missed out, where you think additional safety measures are required or if there is something we can help you with PLEASE make sure you let us know so we can improve on our policies and processes going forward, **as we said before GDPR is everyone's responsibility…**

What to do now? Read the attached Doorstep Arts Data Protection Policy and then….

Is everything clear, is there anything you are unsure about?
Consider what data you process, what applies to you, and if you comply
Act and put everything in place to make sure you do comply
ASK if there is anything you are unsure about
BRING your ideas to the next meeting
DATA AMNESTY! Clear out all data that is no longer relevant, be it on your laptop or paper-based documentation….
CHECK new processes or actions put in place – have they helped you and what are your comments?

By working with Doorstep Arts you are confirming that you have read and understood the aims and scope of our GDPR Policy and that everything is in place to make sure that you are working within the policy guidelines.

Doorstep Data Protection Policy see pages 4 – 10.

Doorstep Arts Data Protection Policy

Aim

That Doorstep Arts processes personal data fairly and lawfully and in line with the Data Protection Principles

All those working with Doorstep Arts and involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities under this policy.

That the data protection rights of those involved with Doorstep Arts are safeguarded

That there is confidence in Doorstep Arts Ability to process data fairly and securely

Scope

This policy applies to data of all those working for Doorstep Arts, students, parents and carers and any other person carrying out activities on behalf of Doorstep Arts and Board Members and includes the processing of personal data both in manual format and on computer.

Data Protection Principles

Doorstep will ensure that all personal data will be:

1) Processed fairly, lawfully and in a transparent manner
2) Collected for specified, explicit and legitimate purposes and not further processed for other purposes other purposes incompatible with those purposes.
3) Adequate, relevant and limited to what is necessary in relation to the processes for which the data is processed
4) Accurate and, where necessary kept up to date
5) Is kept for no longer than is necessary for the purposes for which the personal data is processed
6) Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, damage and using appropriate technical and organisational measures

Doorstep Arts will be able to demonstrate compliance with these principles and will have a process in place dealing with the following rights in respect of an individual's personal data:

To being informed what data is held, why it is being processed and who it is shared with
To access to relevant data
To Rectification of records
To Erasure
To restriction of processing
To data portability
To object to processing
Not to be subject to automated processing
Profiling

Roles and Responsibilities

The Directors are responsible for implementing good data protection practices and procedures within Doorstep Arts

It is the responsibility of all persons engaged in carrying out activities for Doorstep Arts, employed or self employed to ensure that their working practices comply with the Data protection Principles.

The Data Protection Officer will have responsibility for all issues relating to the processing of personal data and will report to the Directors.

The Data protection Officer will comply with responsibilities under the GDPR and deal with all SARS requests, requests for rectification, erasure, data security breaches.

The Directors are E Walcon, J Campbell, P Ferguson-Carruthers.

The Doorstep Arts Data Protection Officer is Marie Copland

Data Security and data Security Breach Management

All employees or those engaged in work for Doorstep Arts are responsible for ensuring that all personal data that they process is kept securely and not disclosed to any third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All data will be destroyed securely

Doorstep Arts will have a data security management process and all relevant persons will be aware of and follow the data breach security management process (see page 9).

All relevant persons will be aware with the list of Do's and Don'ts in relation to data security, and as recorded within this policy at pages 7 and 8.

Sharing Data with a Third Party and Data Processing Undertaken on Behalf of Doorstep Arts

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Where a third party undertakes data processing on behalf of Doorstep Arts, Doorstep Arts will ensure that there is a written agreement requiring that the data is processed in accordance with the Data Protection Principles.

Ensuring Compliance

All new persons employed by or engaged in work on behalf of Doorstep Arts will be made aware of the data protection requirements.

Photographs, Additional Personal Data and Consents

Where Doorstep Arts seeks consent for the processing of person data such as photographs at events it will ensure that appropriate consents are obtained, these consent forms will also advise how the consent can be withdrawn. Where the personal data involves a person under 16 years written consent will be required from the adult with parental responsibility.

Do's and Don'ts see pages 7 and 8.

a) *Have to renew anti virus office – priced up 10 computers/laptops with MCcaffee small business is £120 for 12 months – this means that all key Doorstep bods have appropriate anti-virus – it also covers unlimited android phones and tablets – is over the top number wise but did not know if worth investigating – would like to renew asap for the office did not know what you thought about multi user…*
b) *Shredder for the office?*
c) *DAS and DYT etc – contact details and medical information is on a paper register printed out each week – can the registers be held on a drop box accessible by relevant person taking session – eliminates necessity to print off and also means updates can be made there and then (monies in/changed contact details) would mean person taking session taking portable device – unsure best way to go? Cheap tablet that could be used for registers and/or evaluation data collection?*
d) *Lockable cabinet for archived tax year records (accounts/registers/general correspondence) tackle filing cabinet in cupboard – office – joint clear out and rejig – maximise space –*
e) *Need all consent forms (overlap DAS and DYT so some info on DAS registers not showing*
f) *Email out DAS/DYT etc– once a year asking if any personal details have changed (contact and medical) and if still happy consent for photographs to be used keeps records up to date – start of every academic year?*

DO….

DO get permission before taking any confidential information home

DO transport information from school on SECURE computing devices – where possible AVOID taking paper documents out of the office

DO use SECURE portable computing devices such as encrypted laptops and encrypted memory sticks when working from home

DO ensure that any information save on a USB, camera, laptop, phone is SECURELY deleted off the device or saved on the Doorstep shared drive

DO ensure that all paper-based information that is removed from the office is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.

DO ensure that any confidential documents that are taken home are stored in a LOCKED drawer.

DO ensure that any paper-based information or laptops are kept safe and close to hand when off premises and never leave unattended, especially in public places. Remember to not read confidential information in places such as public transport.

DO ensure that when transporting documentation in your car that it is locked in the boot in transit.

DO return paper-based information to the office as soon as possible and file/dispose of it securely.

DO REPORT any loss of information (paper based or held on portable computer devices) to the Directors and Data Protection Officer immediately, this INCLUDES the holidays and weekends.

DO ensure that all email and postal addresses are checked to ensure safe despatch – when sending personal information this should be marked Private – Contents of Addressee Only.'

DO ensure when mailing information that ONLY the specific information required by the recipient is sent

DO anonymise personal information where necessary

DO ensure that access to information is restricted to the appropriate people only

DO encrypt documents where necessary

DO make sure you ask if there is anything you are unsure about

DO remove downloads from home PC if working from home

DO set up and maintain a strong password

DO password protect your phone if you use it to access work emails

DO make sure that all information is retained and disposed of in line with appropriate requirements

DON'T

DON'T take confidential information to a public place or social event, any information must be taken to the destination DIRECTLY

DON'T unnecessarily copy other parties into e-mail correspondence – personal emails are classified as personal data

DON'T include full names in subject lines – use initials only

DON'T scan documents to a generic scan mail – use a specified admin one or one that has been specifically set up

DON'T leave confidential documents in general/accessible areas at home or in the office

DON'T make calls to parents or carers in public places – this includes using the office phone to make confidential calls when other unrelated parties may be present

DON'T email confidential documents to a computer that is not a work computer and is not adequately secure

DON'T store work documents on a home computer

DON'T leave unclaimed documents on the printer or copier

DON'T leave personal information on your desk or on your computer when you are away from your desk/the office

DON'T leave documentation in vehicles over night

DON'T discuss confidential matters at social events or in public places

DON'T put confidential documents in non-confidential bins, recycling bins

DON'T print off reports with personal data (e.g. Student data) unless ABSOLUTELY necessary

DON'T use unencrypted memory sticks or unencrypted laptops

Process for Data security Breach Management

EVERYONE working for Doorstep has an INDIVIDUAL responsibility for reporting data loss or security risk IMMEDIATELY

The DPO & Directors must without delay consider and implement appropriate steps to contain or recover the breach, this may include paperwork misplaced or a misspent email.

ALL breaches must be documented – this must include the facts, effects, remedial action taken, see data Breach Reporting Form – page 10.

FURTHER steps and actions to be decided on risk factors to be considered to include emotional distress, physical risk, financial damage, risk of identity fraud. Where a breach has to be reported to the ICO (if applicable) this must be carried out within 72 hours.

The DPO and Directors to review any breach and identify necessary improvements and amend the policy accordingly.

DATED 14TH June 2021

Reviewed June 2024

Data Breach Reporting Form