Data Protection

In accordance with the EU General Data Protection Regulation 2018 (GDPR)

Policy
& Procedure

Updates

Review Date	Page No	Updates	Next Review
30/5/2018		No updates made	01/09/2018
01/09/2018		No updates made	01/03/2019
01/03/2019		No updates made	01/09/2019

Data Protection and Information Security Policy

Overview

Up-Grade Training is committed to ensuring data and information are protected and secure. As an independent Training and Youth Work Company, we process information in both paper and electronic form relating to Young People, Training Participants, Carers and AQA course and exam information.

We also undertake work with My Choice Homes who look after young people ages between 8-18 years, however the average age is 15-18 years. The homes range from 2-4 bedded. The young people who live in their homes have significant emotional and behavioural difficulties, with other educational, social and health concerns, they are all looked after children and have allocated social workers or other professionals involved in their care.

All members of staff receive data protection training at the point of induction and a refresh when necessary. All members of staff are aware of the data protection and information policy.

This policy is designed to ensure compliance with current legislation with respect to confidentiality, accuracy and security of data. It is the responsibility of the Director Daniel Barfoot to ensure that all staff comply with this policy. Failure to comply with this policy may be dealt with under the Up-Grade Training disciplinary procedures.

1. Introduction

1.1. This Policy outlines how we'll:

- Comply with the General Data Protection Regulation (GDPR), Article 8 of the Human Rights Act and any associated case law
- Ensure all staff involved in processing personal information understand their responsibilities.

1.2. The aim of the Policy is to assure the people about whom we hold data, that we'll process and store their personal information in accordance with the GDPR.

1.3. This Policy applies to:

- All Up-Grade Training staff (including permanent, temporary, agency, voluntary, work placement and contract staff)

1.4. Throughout the Policy: the terms 'you' and 'your' mean staff and data processors. The terms 'we', 'our' and 'us' mean Up-Grade Training

1. What is the General Data Protection Regulation?

1.5. The GDPR sets out legal requirements for all organisations processing personal data. The Regulation is designed to give individuals greater control and protection over the use of their personal data.

1.6. Data Protection law is enforced in the UK by the Information Commissioner's Office (ICO). The ICO can impose strong penalties on us if we don't comply with the GDPR, including criminal prosecution, non-criminal enforcement and audit. The ICO can issue monetary penalties of up to 4% of Up-Grade Training annual turnover – or an unlimited fine in a Crown Court.

Failing to comply with our Data Protection Policy and associated procedures could damage our reputation and lead to a loss of trust in our organisation, as well as having a significant adverse financial effect.

2. How will we comply with the Principles of the General Data Protection Regulation?

2.1. We'll comply with the six principles of the GDPR by:

1. Processing personal data fairly, lawfully and in a transparent manner. We'll not process data unless:

a) we've identified a valid lawful basis for processing under Article 6 of the GDPR, and

b) in the case of special categories of personal data, we've also identified a special category condition in compliance with Article 9.

Articles 6 and 9 are available in Appendix One.

2. Obtaining personal data only for one or more specified, explicit and lawful purposes. We won't process any data in a manner incompatible with this purpose or purposes.

We'll never deceive or mislead individuals when we collect their personal information. All forms we use to collect data will clearly state:

- **Who we are**
- **Why we are collecting the information**
- **How we intend to use the information**
- **Where the data subject can find our Privacy Notice**
- **Any other information we feel is useful.**

3. Ensuring the personal data, we hold is adequate, relevant and limited to what is necessary in relation to the purpose for which the data was collected.

4. Ensuring personal data is accurate, and where necessary, kept up to date. If we are made aware the personal data, we hold is inaccurate we will erase or rectify the data within one month.

5. Ensuring personal data is not kept for longer than necessary in relation to the purpose for which the data was collected. We'll securely dispose of any records we no longer need.

6. Implementing appropriate technical and organisational measures to protect data against:

a. Unauthorised or unlawful processing
b. Accidental loss, damage or destruction.

3.2 Accountability Principle

To demonstrate our commitment to GDPR principles and acknowledge Up-Grade Training responsibility to comply we will:

a) Maintain data protection policies
b) Implement mandatory staff training
c) Maintain relevant documentation on processing activities
d) Appoint a data protection officer
e) Adopt the principles of data protection by design and data protection by default, including where appropriate:

3.3 We'll provide a Privacy Notice telling data subjects what to expect when we collect their personal information. The Privacy Notice will state the lawful basis for processing and who we'll share data with. If we make any changes to our notice, we'll immediately publish the changes on our website.

3.4 If there's a change to the type of personal information we collect or the nature of the processing, we'll issue a revised Privacy Notice to all parties who access Up-Grade Training in 3.3. We'll explain the changes, the reason for the changes and the lawful basis for processing.

3.5 There are certain exemptions in the GDPR, which mean there are times when we don't have to comply with the above principles, or with data subject rights. These are used rarely and only in special circumstances. If staff wish to apply a relevant exemption, they must first contact Up-Grade Training Data Protection Officer Daniel Barfoot

3.6 We'll never rent or sell any personal information to third parties.

3.7 Up-Grade Training are not allowed to use personal information for any other purpose than it was obtained, subject to the exemptions in the GDPR, referenced in 3.5 above.

3.8 Before collecting data for a new purpose staff must consult Up-Grade Training. This is because:

- It may be unlawful to use the data for another purpose
- We may need to amend our ICO notification (it's a criminal offence if this isn't accurate)
- We may need to inform data subjects and/or gain their consent.

4 Useful definitions within the GDPR

4.1 Data Subject

A living individual who is the subject of personal data or can be identified from the data. For us this includes past, present and prospective:

- Staff
- Course Participants
- Carers
- Contractors
- Suppliers
- Young people

4.2 Data

- Information stored electronically, e.g. on a computer (on a hard drive or in an email server (such as Outlook)), in a cloud-based database, backed up files, faxes, videos, email, information on telephone logging systems, photographs or text messages

- Information generated using automated means e.g. credit score or profiling

- Manual information recorded with the intention it will be processed electronically – e.g. file notes made by hand, which will later be input online

- Manual Information which is structured and accessible

4.3 Processing

Carrying out any operation or set of operations on our data, including:

a) Collection, recording, organisation, adaptation or alteration of the information or data
b) Retrieval, consultation or use of the information or data
c) Disclosure of the information or data by transmission, dissemination or otherwise making available, **or**
d) Alignment, combination, blocking, erasure or destruction of the information or data.

4.4 Personal data

Data relating to an identifiable person, who can be identified either directly or indirectly (i.e. by reference to an identifier, e.g. location data):

It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.5 Sensitive Personal data

Data relating to someone's:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union membership
- Health
- Sex life or sexual orientation

4.6 Data Controller

The organisation that determines the purpose of the processing, i.e. how the personal data will be used. In our case this is Up-Grade Training.

4.7 Data Processor

Any organisation processing data on our behalf, e.g. contractors.

5 What are our responsibilities?

5.1 The Director is ultimately responsible for compliance with the GDPR

5.2 Up-Grade Training appoint a Data Protection Officer Daniel Barfoot

- Maintain this Policy and any supporting policies and procedures
- Provide data protection guidance and advice to colleagues and residents
- Manage and advise on breaches
- Provide advice to colleagues on Data Protection Impact Assessments when starting new processes or purchasing new software
- Ensure Up-Grade Training and its subsidiaries have accurate and up to date Notifications with the ICO
- Act as the contact point for the ICO
- Provide mandatory training for all new members of staff and annual refresher training for existing staff
- Provide mandatory training for anyone who has access to personal information.

5.3 Up-Grade Training are responsible for implementing this Policy and championing data protection.

5.4 The Up-Grade Training will consider disciplinary action (in accordance with our Disciplinary Policy) against staff who fail to:

- Comply with the GDPR – this includes accidentally, knowingly, or recklessly breaching the Act.
- Comply with their duty of confidentiality as outlined in this Policy
- Comply with our data protection policy and procedures – and any associated policies and procedures.

5.5 All staff have a duty to maintain the security of personal information. Staff must contact the Data Protection Officer if:

- They’re aware of a possible data protection breach
- They’re concerned about the way data is being used within the organisation.

6 Organisational and Technical Security

6.1 Ensuring we keep the personal data we hold secure is fundamental to data protection law. We hold lots of personal and sensitive personal information and have a duty to keep it safe.

6.2 We'll follow the organisation and technical security principles set out in the following policies:

- Physical and Environmental Security Policy
- Acceptable Use Policy
- Protective Marking Guidelines
- Bring Your Own Device Policy Guidelines
- Access Control Policy

7 Individual Rights

The GDPR introduces eight rights for individuals:

7.1 The right to be informed

We'll be open, honest, fair and transparent with individuals about the use of their personal data. We'll provide a Privacy Notice as set out in Section 3.3 and ensure it's drafted in accordance with guidance provided by the ICO.

7.2 The right of access: Subject Access Requests

All individuals have the legal right to ask us if we're processing their personal information. The requests are called Subject Access Requests (SARs).

If we receive a SAR, (or a request that could possibly be one), you must inform the Data Protection Officer immediately, even if it's a verbal request.
We'll comply with SARs in accordance with the GDPR by following our Procedure in Appendix Two. We'll respond to SARs promptly and in any event within 28 calendar days of receiving it.

Any request should be made in writing to;

Mr Daniel Barfoot
Up-Grade Training
50b Sackville Road
Bexhill
East Sussex
TN39 3JE

7.3 The right to rectification

Individuals have the right to ask for their personal data to be rectified if it's inaccurate or incomplete. We will respond to all requests without undue delay and within 28 calendar days

7.4 The right to erasure

Individuals can request the deletion or removal of personal data where there is no compelling reason for its continued processing. We'll consider requests for erasure by following our Procedure in Appendix Two.

7.5 The right to restrict processing

Individuals have a right to 'block' or suppress the processing of personal data. This only applies to Up-Grade Training

- If an individual query the accuracy of their personal data we will restrict processing until we have verified the accuracy of the personal data
- If the processing is unlawful and the individual opposes erasure and requests restriction instead
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim

If we agree with the request to restrict processing of an individual's personal data we will continue to store the personal data, but not further process it.

7.6 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. We'll consider data portability requests by following our Procedure in Appendix Two.

7.7 The right to object

We will notify individuals of their right to object to direct marketing in our Privacy Notice. We will stop processing personal data for direct marketing purposes as soon as we receive an objection and no later than 28 days.

8 Consent

Some of the services provided by Up-Grade Training will rely on consent, for example social media activity.

Where we require consent to provide a service we'll follow the requirements set out in the GDPR. Consent requests will be explicit, transparent and for a specific purpose only. We'll ask individuals to positively opt-in and allow individuals the opportunity to withdraw consent without detriment.

9 Taking files and papers out the office

9.1 We understand it's sometimes necessary to take files and papers out of the office but taking personal data out of its secure place is a serious data protection risk and must be avoided. We'll follow the procedure for taking files out of the office set out in Appendix Three.

10 Disclosing information to other third parties

10.1 There may be occasions where we receive requests to share personal data with a third party with which we don't have an existing relationship. This can involve a one-way disclosure to a third party or a mutual exchange of personal data.

10.2 Generally, the GDPR does not allow us to disclose information to a third party unless

- The data subject has been informed (for example through our Privacy Notice) or has given us their consent. We'll still ensure the disclosure meets one of the conditions in Article 6, and one of the conditions in Article 9 if the data is sensitive information.

- A relevant exemption in the GDPR applies. For example, if the Police need information to prevent or detect crime, safeguarding of a young person or prosecute a suspect.

- We believe sharing the information is in the vital interests of the data subject. This is generally life and death situations only and will be rarely used.

10.3 As a general rule, we'll not disclose information in response to a telephone request from a third party.

We'll always ensure requests for information are received in writing. Requests must be on letter headed paper or sent from a legitimate email address. We may verify the identity of the requestor, for example by contacting their organisation.

10.4 We'll not disclose information to a third party who visits one of our offices without prior arrangement.

If the request is urgent (for example Police visit our office reception) staff must contact the Director Daniel Barfoot.

10.5 We'll ensure the third party agrees to return, or securely destroy the information we send when they no longer need it.

10.6 All disclosures to a third party must be authorised by a senior manager or the Data Protection Officer. The reason for the disclosure decision must be recorded in writing and emailed to the Data Protection Officer within three days.

We'll decide if the disclosure is appropriate. Even it is a valid request, we will consider whether there is a more appropriate source of the information.

We'll only share the minimum amount of information required. We'll record the disclosure on the data subject's file.

11 Information Sharing Agreements

11.1 When we engage in regular sharing arrangements with a third party we'll ensure both parties sign an Information Sharing Agreement. These ensure we share certain routine information legally. Before sharing any information under an Information Sharing Agreement we'll:

- Ensure the agreement covers the type of information we want to disclose
- Follow the specific procedure or authorisation process (outlined in the Operating Regulations) to ensure we share data fairly and lawfully.

12 Using Personal Information in Corporate publications or on our website

We'll always obtain explicit signed consent from the data subject, before we publish any personal information. This includes photos taken at social and training events.

13 Data Protection Breaches

13.1 In the event of a data protection breach, staff must refer to our Data Protection Breach Procedure.

13.2 All staff are responsible for reporting data protection breaches to the Data Protection Officer as soon as possible. But no later than 24 hours after the breach is detected.

14 Information relating to people who have died /moved on

14.1 Although the GDPR only applies to living individuals, staff must apply the same level of confidentiality to a deceased person's information, as they would to a living person's information.

14.2 If a young person transfers from My Choice Homes to another home within the company or external to the company, their records and other data that related

to their health, education and welfare will be forwarded onto the placement. This will support a smooth transition from one placement to another and ensure that the young person is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the young person's progress as a result of the move.

15 Data Protection Impact Assessments (DPIAs)

We'll consider the potential impact of new initiatives and change on individual privacy and adopt a privacy by design and default approach.

New initiatives which will involve the use of personal data will require a Data Protection Impact Assessment, this will include:

- New or significant change to IT systems storing personal data
- Any changes to how we share or manage personal data e.g. a new Assessment Form
- Policy reviews resulting in new ways of managing personal data.

Staff responsible for managing the project / change must complete a DPIA before the project starts. The completed DPIA will be reviewed by the Date Protection Officer

16 Confirming Identity of telephone callers

All Staff must follow the security procedures set out in Appendix Four to confirm the identity of telephone callers.

Each caller will have slightly different needs for questions and the Staff member or Carer can choose the most suitable. Questions must be things where there is a strong likelihood only the Data Subject will know the answer. Any change to the agreed security questions must be approved by the Data Protection Officer.

17 Review

We'll review this Policy annually, or sooner to include legislative, regulatory, best practice development or to address operational issues.

APPENDIX 1

Lawful Basis for Processing – Articles 6 and 9

When we process personal data we must meet certain conditions set out in the GDPR. When we process:

- **Personal Data**, we must meet one condition in Article 6 of the GDPR.
- **Sensitive (special categories) of Personal Data**, we must meet one condition in Article 6, and one condition in Article 9 of the GDPR.

Article 6

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

Article 9

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Human Rights Act Article 8

If the information shared is of a private nature (e.g. family life) it must meet one of the following criteria – and it must be necessary and proportionate to share.

- Interests of national security
- Public safety
- Economic well-being of the country
- Prevention of crime and disorder
- Protection of health and morals
- Protection of the freedom and rights of others

APPENDIX 2
Procedure for Subject Access Requests

Everyone has the right to see the information Up-Grade Training holds on them (this includes paper and computer files) – this is called a Subject Access Request (SAR).

There is no charge for this request. We'll provide the information without delay and at the latest within 28 days of receipt.

Before providing the information, we'll ask the individual to confirm:

- their identity by providing two forms of photocopied identification
- how they would like to receive the information (by paper or electronic copy)

Where requests are manifestly unfounded or excessive, because they are repetitive, we may:

- charge a reasonable fee considering the administrative costs of providing the information; or
- refuse to respond.

Where we refuse to respond to a request, we'll contact the individual within one month explaining our reasons for refusal and their right to complain to the ICO.

SAR requests for Training Participants will be dealt with by Up-Grade Training

SAR requests for staff (former and current) will be dealt with by Up-Grade Training

Procedure for Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data must be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

We will refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- 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.
- the exercise or defence of legal claims.

Procedure for Data Portability Requests

Other Agencies or Local Authorities will be given the ability to view their data from Up-Grade Training Database

This will only be done for specific staff when we receive requests in writing. We will require:

- Two verifiers
- A description of the data we are requested to provide

We will provide the information within 28 days. We will arrange a time and place for the file to be viewed.

It's a requirement of the GDPR that the data we hold is accurate and up-to-date. To ensure the data meets our requirements and is not in breach of the GDPR we will obtain data directly from carers to verify their Identity.

Appendix 3

Procedure for taking files and papers out of the office

Where it's necessary to take files and papers out the office or home, staff and must follow these guidelines:

- A log must be made in an agreed register/system (see below for the types of documents this applies to)
- Take only the information you need – the absolute minimum.
- Consider the risks!
- Make documents as anonymous as possible. For example, remove visible names, addresses, date of births etc. And any identifiers.
- Never leave a work case or bag unattended. Be particularly wary at transport hubs, on public transport and at eateries. Buying a ticket or having a meal are ideal opportunities for a thief to steal a bag.
- Remember a car is not secure. Never leave personal information in a car. Not even in the boot.
- Return the documents at the earliest opportunity. Ideally, this will be the same day.
- Keep documents taken home or to other people's homes overnight safe, secure and confidential.
- Update your register/system once documents are returned.
- Never dispose of documents at home.

The following documents must be signed out:

- Any documents which contain more than basic personal information. For example, a form which contains someone's name, address, NI number and date of birth. If lost, this information could be used for identity theft. We must inform the relevant parties.
- Several documents about the same person.
- Documents containing sensitive information (list below).

Sensitive Data according to the Act is data relating to someone's:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

Appendix 4

Procedure for Confirming Identity of Telephone Callers

All Staff Members and Carers must use an agreed list of security questions to ensure a caller is who they say they are before having any conversations that involve sharing personal Data. Before disclosing any personal information, a caller must answer three questions chosen at random from the list below:

- Password (if they've set one)
- National Insurance Number
- Name of First Placed Child
- Child or Carers DOB
- Amount of last allowance payment made
- Childs NI number
- Childs LA identifiable/reference Number
- Date Current Child was first Placed
- Child or Carers Middle name
- What is your normal payment method?

Residents may authorise third parties to contact us on their behalf, using authorised written consent

If the third party is a Local Authority, use the questions above to identify them. If the third party is not a Local Authority use the questions below:

Information provided to us in written consent:

- Postcode (of third party)
- Telephone number (of third party)

Plus at least one of the questions below:

- Password given to them and provided in written consent (by Foster Carer)
- National Insurance (NI) Number (of Foster Carer).

If the staff member is unable to confirm the identity of the caller after answering the questions, the information that the caller has requested will not be provided until the questions can be answered.

If the staff member needs to transfer the caller to another staff member then they must also confirm the outcome of the verification process.

Each caller will have slightly different abilities to answer the questions and the Staff Member or Carer taking the call can choose the most suitable. Questions must be things where there is a strong likelihood only the data subject will know the answer. Any change to these questions must be approved by the approval of the Data Protection Officer, Daniel Barfoot.