POLICY:	Data Protection (incorporating GDPR and DPA 2018)
STATUS :	Final
AUTHOR(S):	Tess Gregson
DATE:	10/3/2010
CIRCULATION:	External
REVIEW DATE	April 2013; October 2014; November 2015; March 2016; March 2017; March 2018; May 2018; Apr 20
NEXT REVIEW	Apr 2021
SEE ALSO:	• E-Safety Policy • Case Recording & Information Policy & Procedures • Information Governance Policy • Network Security Policy • Data Protection Impact Assessment (DPIA) Template and Map • Confidentiality policy • Serious Untoward Incident Policy and Report Form • Monitoring and Evaluation Policy & Procedures • Young people's Policy Information Leaflets

1.0 Introduction

1.1 42nd Street is committed to protecting the rights and privacy of individuals including: trustees; staff; those who apply for vacancies as part of recruitment processes; those employed by 42nd Street past and present; young people past and present that both contact and engage in our service; and any volunteers, partners, donors, and members, in accordance with the General Data Protection Regulation 2018 (GDPR). We shall ensure that all staff that has access to any personal and/or sensitive data held by or on behalf of 42nd Street is fully aware of and abides by its duties and responsibilities under the GDPR.

2.0 Statement of policy

2.1 In order to offer a high-quality service to young people, 42nd Street collects and uses information about the people with whom it works. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly in whatever way it is collected, recorded and used, for e.g. on paper, in electronic records or recorded by any other means, and there are safeguards within the Act to ensure this.

2.2 42nd Street regards the lawful and correct treatment of personal information as implicitly important to its successful operations and to maintaining confidence between the organisation and those with whom we work. 42nd Street will ensure that it treats personal information lawfully and correctly.

2.3 In forming contracts with third parties, whether they are individuals contracted to work with 42nd Street, services or other third parties, it will be a stipulation of the contract that all third party representatives with access to personal data will be expected to read and comply with this policy. It is expected that any staff whose responsibility it is to negotiate and agree contracts which commit 42nd Street to undertake any joint working alongside external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to adhere to this policy. Some Service Level Agreements may make specific arrangements unique to the type and nature of service, where 42nd Street is the service provider. For example, an SLA with a school may identify that 42nd Street will observe the school confidentiality and safeguarding

policies and procedures but that in some cases 42nd Street may refer to its organisational policy.

2.4 Any breach of GDPR or 42nd Street's Data Protection Policy will be considered an offence and in that event, 42nd Street disciplinary procedures will apply. 42nd Street will report any data breaches or near misses in accordance with its Serious Untoward Incident (Information incidents) policy and procedures and in accordance with statutory procedures.

3.0 Legal Requirements and Application of the legislation

3.1 Data is protected by the General Data Protection Regulation (GDPR). The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018. These supersede the Data Protection Act (1998). Its purpose is to protect the privacy and rights of individuals to ensure that personal data is not processed without their knowledge, and, wherever possible, is not processed without their consent. Processing in this policy will relate to collecting, storing, amending, sharing, and erasing of data. GDPR extends previous legislation regarding consent, and places significant emphasis on transparency and the right of the individual to be informed of their rights and their need to pro-actively to consent to the purposes for which their data is held and processes.

3.2 The GDPR applies to data 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. 42nd Street both acts as a data controller in some contexts and processes data in the course of its work.

3.3 As a processor, the GDPR places specific legal obligations on 42nd Street; for example, the Charity is required to maintain records of personal data and processing activities. 42nd Street will have legal liability if the Charity is responsible for a breach.

3.4 As a data controller, where a processor is involved, the GDPR places further obligations on 42nd Street to ensure our contracts with processors comply with the GDPR.

3.5 The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

3.6 The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

3.7 GDPR was developed by the EU's Article 29 Working Party – which has now been renamed the European Data Protection Board (EDPB). The EDPB includes representatives of the data protection authorities from each EU member state. In the UK, the Information Commissioner's Office is the UK supervisory authority.

3.8 In accordance with the statutory requirement of any body which processes personal data, 42nd Street is registered with the Information Commissioner's Office (Registration Number: ZA193919).

3.9 42nd Street's registered Data Protection Officer (DPO) is Tess Gregson, Head of Business Operations.

4.0 The 7 Principles of GDPR

4.1 Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

4.2 Article 5(1) requires that personal data shall be:

- "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

4.3 Article 5(2) adds that:

- "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

4.4 It should be noted that when read in the context of the previous DPA (1998) which set out 8 principles of data protection, the following changes are relevant within GDPR:

4.4.1 Individuals' rights are dealt with separately in Chapter III of the GDPR;

4.4.2 There is no principle for international transfers of personal data. This is now dealt with separately in Chapter V of the GDPR; and

4.4.3 There is a new accountability principle. This specifically requires you to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply. There is now a clear emphasis on a controller being able to strongly evidence their systems and practices in relation to GDPR.

5.0 Personal and Sensitive Data

5.1 GDPR and DPA 2018 provide conditions for the processing of any personal data. It also makes a distinction between '**personal data' and 'sensitive' personal data**.

5.1.1 '***Personal data***' is defined as: ***'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'***

5.1.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

5.1.3 The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. In the context of 42nd Street, one example of this is our use of both electronic case records and hard copy case files.

5.1.4 Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

5.1.5 The GDPR refers to ***sensitive personal data*** as ***"special categories of personal data"*** (see Article 9).

5.1.6 Examples of sensitive data include: ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; gender identity; sexual orientation. The special categories specifically now also include genetic data, and biometric data where processed to uniquely identify an individual.

5.1.7 Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

6.0 Purposes for which data is held

6.1 42nd Street holds data for the following purposes:

- Staff administration
- Fundraising
- Realising the objectives of a charitable organisation or voluntary body
- Accounts and records
- Advertising, marketing and public relations
- Education
- Health administration and services including national NHS data submissions
- Information and data administration

7.0 The Lawful Basis for Processing

7.1 You must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing which are set out in Article 6 of the GDPR. At least one lawful basis must apply whenever data is processed:

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

2. 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.

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

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

5. 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.

6. 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.

7.2 42nd Street recognises that informed consent enables young people, particularly those who may experience disadvantage or who experience mental health difficulties, to have real choice and control in their engagement at 42nd Street. Genuine informed consent is a central ethos of a young person-centred service and builds trust and engagement, and enhances confidence in our services and enhances our wider reputation.

7.3 In the delivery of direct support to young people, with the purpose of health administration and services, 42nd Street's lawful basis is consent and we take informed consent extremely seriously. We take a systematic approach to the process of consent and individual rights connected with this.

8.0 Individual Rights

8.1 The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

8.2 The ICO has created the table below to provide clarity about the types of privacy information which should be provided to individuals, whether collected from the individual or from another source:

What information do we need to provide?	**Personal data collected from individuals**	**Personal data obtained from other sources**
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓

The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

8.3 42nd Street provides young people and referrers with clear information at the point of referral and no young person may be accepted into the service without full prior consent to a referral being made. Upon referral acceptance, all young people are provided with a hard copy 'Welcome Pack' which includes information leaflets and service information. This includes specific information leaflets with regard to confidentiality and to data protection, their rights and privacy. At the point of assessment, informed consent is again sought. 42nd Street views the process of consent as a live agreement between those taking up our services and 42nd Street.

8.4 Consent is always sought for the use of (moving) images, and the specific purposes for which they are consented to be used. Signed documentation is always kept securely and a young person is made aware that they can withdraw consent at any time, and how to make this request to 42nd Street.

8.5 There may be times during the course of 42nd Street's work with young people that 42nd Street has a legal obligation, or it is deemed to be within the auspices of a 'vital interest' to share information about a young person without their consent. One example of this may be in relation to safeguarding a young person. Further details of such instances can be found within our Safeguarding Child (Young Person) Policy and Safeguarding Vulnerable Adults and Confidentiality Policy. These policies in connection with systematised forms and templates for recording consent are used throughout the organisation. For example, Information Sharing Consent, Use of Image Consent or Communication type consent. As is best practice where it is reasonably possible to do so, we would work alongside the young person to also consent to this process but in some cases, this may not be possible.

8.6 Consent is also central to our advertising, marketing and public relations. We will never sell, or pass on to third parties any data which is shared by donors, supporters, partners or young people for the specific purpose which they consent to us using data for. All newsletters or wider communications are sent to individuals who have pro-actively opted-in to receive communications from us and via the method identified by the individual.

8.7 42nd Street regularly reviews its consent practices and existing consents to ensure accuracy and that information is always contemporaneous and correctly processed. When a new service or partnership is set up, 42nd Street will review its consent arrangements and provide for the specific purposes and lawful basis on which data is processed. This will be communicated clearly, and in a way that can be readily understood by young people, and others at whom the service is targeted. Consent will always be sought in the form of explicit opt-in by the service user.

8.8 In cases where a young person wishes to make a 'subject access request' and access the data 42nd Street holds about them, we have a clear process for doing this which is communicated to young people in our Data Protection leaflet, available as part of our young people's 'Welcome Pack', as individual hard copy leaflet and as a download on our website. The full process is detailed within our case information and recording Policy.

8.9 The key principles we follow in managing 'subject access' requests (Article 15, GDPR) are as follows:

- All individuals have the right to access their personal data.
- Individuals can make a subject access request verbally or in writing.
- 42nd Street will respond to any request within the statutory one month of receipt of the request.
- 42nd Street will never charge a fee to young people to deal with a subject access request.
- Young people are welcome to make a request via any member of 42nd Street staff.
- 42nd Street will always fully support young people in the process of subject access requests and our practice is to support young people through this, particularly where they are accessing their case file. 42nd Street recognises that reviewing material concerning distressing experiences in their lives can be distressing at the time of access.

9.0 Handling of personal/sensitive information

9.1 42nd Street will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used e.g. information leaflets for young people;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred outside of the European Economic Area (EEA);
- Ensure that the rights of people about whom the information is held can be fully exercised under the GDPR.

9.2 42nd Street will also ensure that:

- At Governance level, there will always be a suitably experienced, knowledgeable and trained identified Information Governance Lead who will support the executive member who is responsible at an operational level. The current Information Governance Lead at Board level is Richard Spearing.
- The Head of Business Operations will lead on and have responsibility for data protection in the organisation;
- All staff handling personal information understand that they have a responsibility to follow good data protection practice;
- All staff managing and handling personal information are appropriately inducted and receive suitable, ongoing annual training;
- All staff complete NHS Digital Training units relating to Data Security Awareness;
- All staff managing and handling personal information are appropriately supervised;
- All staff, students, volunteers, trustees, general public, partners and young people wanting to make enquiries about the handling of personal information have access to appropriate guidance;
- Queries about handling of personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement that sets out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
- All trustees are to be made fully aware of this policy and of their duties and responsibilities under the Act.

9.3 All managers and staff will take all reasonable steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

- Personal data held on computers and computer systems is protected by the use of secure passwords;

- Individual passwords on desktop PCs and laptops are changed automatically and are set to ensure that a suitable level of security is required when individuals select a new password using multiple character types and case sensitive entry. All smart phones are provided to staff with secure access passwords enabled. This feature must not be disabled by individual staff members.

- Data processed on the organisational database (PCMIS system) is subject to a contract with PCMIS which stipulates significant assurances and systematised security protocols to ensure appropriate standards of information security and protection. Staff access to this system is subject to strict multi-layered protection, firewalls, subject access rights and a full clinical audit trail is present within PCMIS.

9.4 42nd Street's Network Security Policy and our Information Governance Policy deal with matters of data security from a systems and network perspective, linking this to staff practice. It is essential that the Data Protection Policy is read in conjunction with the aforementioned policies.

10.0 Implementation

10.1 All managers will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Head of Business Operations. The Head of Business Operations in partnership with the Facilities Officer will also have overall responsibility for:

- The provision of data protection training where required, for staff within the organisation;

- For the development of best practice guidelines;

- For carrying out Data Protection Impact Assessments (DPIAs) within the organisation. All DPIAs will always be signed off by the Information Governance Lead. Full details of 42nd Street's DPIA procedure and action map can be found in our Information Governance Policy.

- For carrying out compliance checks to ensure adherence, throughout the organisation, with the GDPR and DPA 2018.

- The updating of ICO Registration and any amendment to the identified DPO for the Charity.

10.2 The GDPR requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. To this end all managers will be responsible for notifying and updating Head of Business Operations of the processing of personal data, within their area of responsibility.

11.0 Data Breaches and Reporting

11.1 Data breaches and near misses will always be managed in accordance with 42nd Street's Serious Untoward Incidents (Information Incidents) Policy and procedures, and use the appropriate organisational report form. All breaches and near misses will be reported to the

Information Governance Lead, who will then ensure that external reporting procedures are complied with.

11.2 The GDPR now enforces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible.

11.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

11.4 42nd Street ensures it has robust breach detection, investigation and internal reporting procedures in place. The SUI (Information Incidents) Policy, Procedures and Report Form provide a clear framework for actions to be taken and external reporting procedures, including timeframes within which these must be completed. This facilitates decision-making about whether or not 42nd Street needs to notify the relevant supervisory authority and the affected individuals.

11.5 There is a strong emphasis on learning from incidents to ensure change happens as a result to avoid similar incidents occurring in the future. 42nd Street keeps a record of any personal data breaches, regardless of whether or not we are required to notify.

11.6 In relation to clarity as to when the ICO should be notified, the ICO state:

'When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.' (ICO website)

12.0 Data retention periods

Data Type	Period of Retention
Contracts with customers	6 years
Rental Agreements	6 years
Property Leases	15 years

Company Accounts	6 years
Payroll records	6 years
Expense accounts	6 years
Bank records	6 years
Insurance Policies	3 years after lapse
Claims correspondence	3 years
Employers Liability Insurance certificates	40 years
Donations information	6 years
Deeds of covenant	6 years
Personnel records	25 years after employment ceases
Application for jobs where applicant unsuccessful	1 year
Sickness records	3 years
H&S records	3 years
Accident reports	3 years after settlement
Accident Book reports	3 years
Case files & information on service users	25 years