DATA PROTECTION, INFORMATION SHARING AND RECORDING

References

Information Commissioner's Office: Information for Organisations

Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers

1. Data Protection

1.1 Introduction

The Guardian Family Network (GFN) must collect, use and retain (up until the student turns 25, or 7 years after termination of our services) information about people with whom it works. This includes:

- children and their families who use the service, including those who are no longer on placement;
- current, past and prospective staff; and
- suppliers.

In addition, it may be required to collect and use information in order to comply with the requirements of central government, such as information to be provided for a Serious Case Review.

GFN must comply with the requirements of data protection legislation. Existing legislation that sets out clear rules around how personal data should be processed will change on 25 May 2018, when the European Union's General Data Protection Regulation (GDPR) comes into force. The detail of the application of the GDPR in the UK is contained in a new Data Protection Bill currently progressing through Parliament (see Section 2, Legislation).

Personal information must be handled and dealt with in accordance with legislation however it is collected, recorded and used; whether it be on paper, on computer or digital records, or recorded in any other way.

GFN must ensure through its procedures and working practices that all employees, contractors, consultants, suppliers and partners who have access to any personal data held by or on its behalf, are fully aware of and abide by their duties and responsibilities under the GDPR.

1.2 Legislation

1.2.1 Data Protection Bill

When the Data Protection Bill becomes law, it will replace the Data Protection Act 1998. The Bill aims to ensure that UK data protection legislation keeps pace with technological change, and the impact that has on the collection and use of personal data. It also ensures that the standards set out in the GDPR are implemented in the UK; these are stricter than current DPA legislation.

In addition to governing general data covered by GDPR, the Bill covers other general data, law enforcement data and national security data. It introduces a number of agreed changes to the GDPR to make it work for the benefit of the UK in areas such as child protection, academic research, and financial services.

1.2.2 General Data Protection Regulation

The GDPR is a European regulation which intends to strengthen and unify data protection for all individuals (the data subjects) within the European Union (EU). It also includes the export of personal data outside the EU. It aims to give back control of their personal data to citizens and simplify the regulatory environment for international business. It comes into force on 25th May 2018.

The regulatory detail will not change once Britain leaves the EU in 2019; it is incorporated in the Data Protection Bill.

The main reasons for introducing the GDPR include:

- outdated legislation which is out of step with technological advances;
- an inconsistent approach in different EU countries to data protection;
- limited control for individuals, as data subjects;
- limited rights for data subjects;
- a lack of security and privacy in product development (for example, website design).

In order to tackle these concerns therefore, the GDPR:

- stipulates that each EU member must abide by the regulation and by any business that trades within the EU or with EU data;
- aims to create a consistent environment throughout Europe and beyond to enable the secure flow of data;
- gives individuals greater control of their data by improving consent processes;
- introduces the ‘right to be forgotten’ which enables the data subject to have their data ‘forgotten’ once it is no longer being used for the purpose which it was collected. The ‘right to data portability’ allows individuals to acquire and reuse their personal data across different services.

1.3. Principles of Data Protection

Under current legislation, the DPA 1998 states that anyone processing personal data must comply with eight principles that are laid down in the legislation. These are legally enforceable and require that personal information:

1) shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2) shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4) shall be accurate and where necessary, kept up to date;
5) shall not be kept for longer than is necessary for that purpose or those purposes;
6) shall be processed in accordance with the rights of data subjects under the Act;
7) shall be kept secure that is, protected by an appropriate degree of security;
8) shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Under the Data Protection Bill, these principles and safeguards will be amended to six. These are:

1) processing must be lawful and fair;
2) purposes of processing must be specified, explicit and legitimate;
3) personal data must be adequate, relevant and not excessive;
4) personal data must be accurate and kept up to date;
5) personal data must be kept for no longer than is necessary; and
6) personal data must be processed in a secure manner.

1.3.1 Handling personal or sensitive information

Current and proposed legislation outlines conditions for the processing of personal data and makes a distinction between personal data and sensitive personal data.

Personal data is defined as data relating to a living individual who can be identified from that data; and other information which is in the possession of or is likely to come into the possession of the data controller. This includes an 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.

Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or other beliefs;
- trade union membership;

- physical or mental health or condition;
- sexual life;
- criminal proceedings or convictions.

1.4. Data Protection Practice

1.4.1 Current practice

GFN must:

- 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;
- 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 abroad without suitable safeguards;
- ensure that the rights of people about whom the information is held can be fully exercised under data protection legislation.

These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information;
- the right to prevent processing in certain circumstances;
- the right to correct, rectify, block or erase information regarded as wrong information.

In addition, the service will ensure that:

- there is someone with specific responsibility for data protection in the service;
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- queries about handling 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, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All GFN staff should be aware of this policy and of their duties and responsibilities under data protection legislation. They should take 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, which (where possible) have forced changes periodically;
- individual passwords should be such that they are not easily compromised.

All GFN contractors, consultants, suppliers and partners must:

- ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the DPA. Any breach of any provision of the DPA will be deemed as being a breach of any contract between the company and that individual, partner or firm (see Report a Breach, Information Commissioner's Office https://ico.org.uk/for-organisations/report-a-breach/);
- allow data protection audits by the company of data held on its behalf (if requested);
- indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors and suppliers who use personal information supplied by the service will be required to confirm that they abide by the requirements of the DPA in relation to such information supplied by the service.

1.4.2 Forthcoming additions to current practice

In addition, from 25th May 2018, GFN must:

- ensure data subjects are given greater control of their data by improving consent processes. Consent must be freely given, specific, informed and a clear indication of their wishes. This must be provided by a statement or clear affirmative action, signifying the individual's agreement to the processing of their personal data;
- must ensure that data subjects have the 'right to be forgotten' which enables them to have their data 'forgotten' once it is no longer being used for the purpose which it was collected. The 'right to data portability' also allows individuals to acquire and reuse their personal data across different services;
- keep a record of data operations (mapping data flow within GFN) and activities and assess if it has the necessary data processing agreements in place, and take action to remedy if not;

- carry out privacy impact assessments (PIAs) on its products and systems;
- designate a data protection officer (DPO) if applicable to GFN;
- review processes for the collection of personal data;
- be aware of the duty to notify the Information Commissioner's Office of a data breach (the relevant supervisory authority);
- ensure 'privacy by design' and 'privacy by default' in new products (such as a new case recording system) and assess whether existing products used by the organisation meets the new data protection standards and take action accordingly to ensure compliance.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start for example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Such systems should automatically provide privacy by default, rather than requiring activation by the user.

2. Information Sharing and Confidentiality

2.1. Introduction

GFN staff and primary carers need to be confident about their responsibilities concerning information sharing.

There is an expectation that from their first point of contact with GFN, children and their parents will be helped to understand the information that is being gathered, processed and stored in relation to them and give their written consent to this. They also have a right to know if and when information held about them is going to be shared, for what purpose it will be shared and with whom (unless there is justified reason to share without informing the child and their parents – see Safeguarding Children from Abuse and Neglect).

There are certain circumstances when sharing information is not appropriate and doing so can cause detriment to children, their parents and the service. Equally not sharing information can have serious consequences, therefore all staff must use their professional judgement on a case by case basis, and if necessary seek help from the manager / Designated Safeguarding Officer (DSO) before making a decision. All decisions and outcomes need to be recorded appropriately (see Section 3, Recording). The most important consideration is whether sharing information is likely to safeguard a child who is suffering or likely to suffer significant harm.

Where information sharing is carried out as part of integrated, multi-agency care and support services, there will usually be a local information sharing agreement that sets out

the procedures and working practices specific to the service. This can be accessed via the Local Safeguarding Children Board's procedures.

2.2. Principles of Sharing Information

These principles are intended to help staff and primary carers share information between organisations:

- **Necessary and proportionate:** When taking decisions about what information to share, staff should consider how much information they need to release. UK data protection legislation requires staff to consider the impact of disclosing information on the information subject and any third parties. Any information shared must be proportionate to the need and level of risk.
- **Relevant:** Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make sound decisions.
- **Adequate:** Information should be adequate for its purpose and the right quality to ensure that it can be understood and relied upon.
- **Accurate:** Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.
- **Timely:** Information should be shared in a timely fashion to reduce the risk of harm. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm to a child. Staff should ensure that sufficient information is shared, as well as consider the urgency with which to share it.
- **Secure:** Information must be shared in an appropriate, secure way. Staff must always follow this policy on security for handling personal information.
- **Record:** Information sharing decisions should be recorded, regardless of whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the person making the request.

2.3 Seven Rules for Sharing Information

1) UK data protection and human rights legislation are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
2) Be open and honest with the child (as appropriate) and their parents from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3) When staff are sharing or requesting personal information from someone, they should be certain of the basis upon which they are doing so. They should seek advice if in any doubt about sharing the information concerned, without

disclosing the identity of the individual where possible (see Section 2.4 Confidentiality).

4) Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Staff may still share information without consent if, in their judgement, there is good reason to do so, such as where safety may be at risk. Staff will need to base their judgement on the facts of the case. However, if they know from the outset that they intend to share information without consent, they should be honest about this where possible and not give a false impression that the person has a choice.
5) Consider safety and wellbeing – staff should base their information sharing decisions on considerations of the safety and wellbeing of the child and others who may be affected by their actions.
6) Necessary, proportionate, relevant, adequate, accurate, timely and secure: Staff should ensure that the information they share is necessary for the purpose for which they are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7) Staff should keep a record of their decision and the reasons for it – whether it is to share information or not. If they decide to share, then record what they have shared, with whom and for what purpose.

A checklist guide on When and How to Share Information is included in this policy at Appendix 1.

2.4 Confidentiality

Information be kept confidential and should:

- only be shared on a 'need to know' basis when it is in the interests of the child / parents;
- confidentiality must not be confused with secrecy;
- informed consent should be obtained but, if this is not possible and other individuals are at risk of abuse or neglect, it may be necessary to override the requirement; and
- it is inappropriate for GFN staff and primary carers to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other children may be at risk.

Where a child or their parents have not given consent to information being disclosed for these purposes, then staff / primary carers – in conjunction with the manager / DSO – must consider whether there is an overriding public interest that would justify information sharing (for example because there is a risk that others are at risk of serious harm). In many cases, the public interest arguments will be clear, and staff should feel confident to share or not to share.

Decisions about who needs to know and what needs to be known should be taken on a case by case basis, in relation to this policy and the legal framework.

Principles of confidentiality designed to safeguard and promote the interests of children should not be confused with those designed to protect the management interests of an organisation. These have a legitimate role but must never be allowed to conflict with the welfare of a child. If it appears to a member of staff that such confidentiality rules may be operating against the interests of the child, they should raise it with the manager / DSO. (See also Whistleblowing).

3. Recording

Information must be recorded by GFN staff on receipt of referral of the child for placement and all placement documentation completed as required by the organisation.

Once a child is on placement, staff and primary carers should be given clear direction by the manager as to what information should be recorded and in what format.

At a minimum there should be a record of:

- date and key events;
- date and circumstances of concerns and subsequent action taken;
- decision making processes and rationales;
- any risk assessments and risk management plans;
- consultations and correspondence with key people;
- any additional support arrangements for the child planned and put into place;
- any safeguarding plans;
- feedback and views of the child and their parents;
- any differences in professional opinion;
- any referrals to professional bodies including date.

Outcomes of the above should also be recorded.

The following should also be adhered to:

- records must be legible and if written should be in black ink;
- any alterations to records must be made by drawing a single line through the word, and correction fluid must not be used;
- entries should be dated and signed, and time of recording noted;
- records should be written with the readership in mind. They should be easy for the child and their parents to read and understand;
- language should be plain, clear and respectful, keeping jargon and to a minimum;
- there should be a clear link between evidence recorded and actions planned / recommended;
- records should be securely stored as outlined in Section 1, Data Protection. This includes at the primary carers home.

Other matters

If you are not happy with our privacy policy

If you are not happy with our privacy policy or if have any complaints, then you should tell us.
If a dispute is not settled then we hope you will agree to attempt to resolve it by engaging in good faith with us in a process of mediation or arbitration.

If you are in any way dissatisfied about how we process your personal information, you have a right to lodge a complaint with the Information Commissioner's Office. This can be done at https://ico.org.uk/concerns/

Compliance with the law

Our privacy policy has been compiled so as to comply with the law of every country or legal jurisdiction in which we aim to do business. If you think it fails to satisfy the law of your jurisdiction, we should like to hear from you.

Review of this privacy policy

We may update this privacy notice from time to time as necessary. The terms that apply to you are those posted here on our website on the day you use our website. We advise you to print a copy for your records.

If you have any questions regarding our privacy policy, please contact us
head@guardianfamily.co.uk

Appendix 1 When and How to Share Information Checklist

1. When

When asked to share information, staff should consider the following questions to help them decide if and when to share. If the decision is taken to share, they should consider how best to effectively share the information.

Q1. Is there a clear and legitimate purpose for sharing information? (This includes taking action in relation to safeguarding children and adults.)

Yes – see Q.2;
No – do not share.

Q.2 Does the information enable an individual to be identified?

Yes – see Q.3;
No – staff can share but should consider how.

Q.3 Is the information confidential?

Yes – see Q.4;
No – staff can share but should consider how.

Q.4 Does the member of staff have consent?

Yes – they can share but should consider how;
No – see Q.5.

Q.5 Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?

Yes – staff can share but should consider how;
No – do not share.

2. How

- Identify how much information to share;
- Distinguish fact from opinion;
- Staff should ensure they are giving the right information to the right individual;
- Staff should ensure they are sharing the information securely;

- Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm.

If at any stage staff and primary carers are unsure about how or when to share information, they should seek advice from their manager / DSO and ensure that the outcome of the discussion is recorded.