Shropshire Strengthening Families through Early Help

Information Sharing Agreement

Legislation

Data Protection Legislation

Data Protection legislation is not about preventing the sharing of personal information provided the required conditions are met, sharing is perfectly legal. Data Protection Legislation comes in many forms, but essentially, it is about governing the collection, use, storage, destruction and protection of a living person's personal data.

This document captures the key areas of legislation that Shropshire Strengthening Families partners rely on to legally share information.

NB Shropshire Council is not responsible for the external website links contained in the following pages.

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Digital Economy Act 2017
- The Freedom of Information Act 2000
- The Local Government Act 1972
- Localism Act 2011
- The Children Act 1989
- The Children Act 2004

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The DPA 2018 is based on 6 principles set out in Section 86 to 91 of the Act.

1. Processing of personal data must be:

(a) lawful, and

(b) fair and transparent.

In order for processing of personal data to be lawful at least one of the conditions in Schedule 9 is met. In the case of sensitive processing, at least one of the conditions in Schedule 10 is also met. Section 86 also considers in determining whether the processing of personal data is fair and transparent, regard is to be had to the method by which it is obtained.

Section 86 also outlines “sensitive processing” meaning;

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data for the purpose of uniquely identifying an individual;

(c) the processing of biometric data for the purpose of uniquely identifying an individual;

(d) the processing of data concerning health;

(e) the processing of data concerning an individual’s sex life or sexual orientation;

(f) the processing of personal data as to—

(i) the commission or alleged commission of an offence by an individual, or

(ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

2. The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

Compatibility is subject to:

> Personal data collected by a controller for one purpose may be processed for any other purpose of the controller that collected the data or any purpose of another controller provided that:
>
> (a) the controller is authorised by law to process the data for that purpose, and
>
> (b) the processing is necessary and proportionate to that other purpose.
>
> > Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing consists of processing for archiving purposes in the public interest, or for the purposes of scientific or historical research, or for statistical purposes. There must also be regard for appropriate safeguards for the rights and freedoms of the data subject.

3. Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data undergoing processing must be accurate and, where necessary, kept up to date.
5. Personal data must be kept for no longer than is necessary for the purpose for which it is processed.
6. Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

General Data Protection Regulation
http://www.legislation.gov.uk/ukpga/1998/29/schedule/1

The key principles of the General Data Protection Regulation (GDPR) are:

> 1. Personal Data must be processed (e.g. collected, held, disclosed) lawfully, fairly, transparently and must satisfy one of the conditions in article 6 of the Regulation. The processing of special category data is further protected in that processing must also satisfy at least one of the conditions in article 9 of the Regulation.

2. Personal Data shall be obtained and processed for one or more specific and lawful purpose(s) and not processed in any manner incompatible.

3. Personal Data shall be adequate, relevant and limited (not excessive) in relation to the specified purpose(s).

4. Personal Data shall be accurate and kept up to date.

5. Personal Data shall not be held for longer than is necessary for the purpose it was collected.

6. Processing of Personal Data must be in accordance with appropriate security, including appropriate technical and organisational measures.

Under article 5 (2) GDPR also requires Data Controllers to be responsible for and able to demonstrate compliance with the principles under article 5 (1), promoting a culture of privacy within organisations.

The first and second principles of GDPR are crucial when considering information sharing. In essence, these require that personal information should be processed lawfully, fairly and transparently and that personal information should only be used for the purpose(s) that it was originally obtained.

Articles 6 and 9 of the Regulation set out conditions that must be met before personal information can be processed lawfully, fairly and transparently. An article 6 condition must be met for all personal information and an article 9 condition must be met when processing special category information.

Article 6 specifies conditions relevant for the processing of any personal data, namely:

- The data subject has given his/her consent to the processing for one or more specific purposes; or
- The processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject prior to entering into a contract; or
- The processing is necessary for compliance with any legal obligation to which the data controller is subject; or
- The processing is necessary to protect the vital interests of the data subject or another natural person where consent cannot be sought physically or legally; or
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party, or parties, to whom the data is disclosed, except

where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It is important to highlight, however, the final condition above does not apply to processing that is carried out by public authorities in the performance of their standard and statutory tasks.

Article 9 specifies additional conditions relevant for the processing of special category data, namely:

The data subject has given his/her explicit consent for one or more specified purposes; or

- 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 obligations; or
- Processing is necessary to protect the vital interests of the data subject or another natural person where consent cannot be given by or on behalf of the individual (physically or legally incapable of giving consent); or
- Processing is carried out in the course of 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; or
- Information already publicly released by the individual; or
- Processing necessary for the establishment, exercise or defence of legal claims; or
- Processing necessary for reasons of substantial public reason; or
- Processing necessary for the purposes of preventative or occupational medicine; or
- Processing necessary for reasons of public interest in the area of public health.

Special category data, as defined by the Regulation, includes information concerning a person's physical or mental health; sexuality; ethnicity or racial origin; philosophical beliefs; political opinion; trade union membership; genetic and biometrics.

Article 44 sets out that personal data should not be transferred to a Third Country without adequate protection as outlined by article 45. A Privacy Seal is required for countries outside of the EEA. Conditions (within Chapter 5 of the Regulation) must be met with to ensure compliance. The following should be taken into account:

a) Rule of law

- Respect for human rights and freedoms

- Relevant legislation

b) Independent supervisory authorities

c) International commitments - The identity and contact details of the controller, and if applicable the representative

In order for there to be no misunderstanding on anyone's part it is always advisable for the 'collector' of the information to ensure that the data subject is made fully aware of why the information is required, what it will be used for, who will have access to it and what their rights are. If appropriate, seek the fully informed consent of the individual concerned before sharing that information.

The Regulation requires Data Controllers to provide a distinct set of information to a data subject when their data is collected. The following should be provided within a Privacy Notice as part of a controllers fair processing obligations:

- The identity and contact details of the controller, and if applicable the representative.
- Contact details of the Data Protection Officer (DPO).
- Purposes of the processing and the legal basis.
- If applicable the legitimate interests pursued by the controller.
- Recipients of the data, if applicable.
- Whether the controller intends to transfer the data to a Third Country and if so what safeguards will be put in place.

It should also be considered that the following is provided:

- The retention period of the data
- Existence of the data subject rights, including the right to access and the right to withdraw consent where applicable
- Information regarding the right to lodge a complaint with the Information Commissioners Office
- Whether the provision of personal data is a statutory or contractual requirement
- If there is any existence of automated decision making, including profiling.

The Regulation gives individuals specific rights in respect of their own personal data held by others, namely the right to:

- Access their information (subject access request)
- Rectify incomplete or inaccurate data
- Erasure (otherwise known as the right to be forgotten)

- Restrict processing
- Data portability
- Object to processing
- Be informed and not subject to decisions solely on automated processing
- Take action for compensation

The right of access gives an individual the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic). Disclosure of information held on an individual's record that identifies, or has been provided by, a third party is subject to certain restrictions.

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/schedule/1

Article 8(1) of the European Convention on Human Rights (given effect via the Human Rights Act 1998), provides that "everyone has the right to respect for his private and family life, his home and his correspondence." This is, however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.

Article 8(2) of the European Convention on Human Rights provides "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s), to have taken a particular course of action:

- That it has taken these rights into account;
- That it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
- If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
- (If qualified rights) Whether the organisation has proceeded in the way mentioned below.

“Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act”.

The Shropshire Strengthening Families through Early Help Information Sharing AgreementI is designed to comply with the provisions of the Human Rights Act 1998 in respect of Article 8 the right to respect for private and family life.

Common Law Duty of Confidentiality

http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/browsable/DH_5803173

All staff working in both the public, private and the third sector should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

‘In Confidence’… Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular were a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

The duty of confidentiality requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and/or has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosures being in the public interest (e.g. to protect others from harm).

Digital Economy Act 2017

http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

The Digital Economy Act 2017 makes provisions about electronic communications infrastructure and services. It contains a suite of measures that will support the digital transformation of government, enabling the delivery of better public services, world-leading research and better statistics.

The Act provides public authorities with new powers to share personal information so they can deliver better support and services which are more tailored to people's needs.

Part 5 Sections 35 – details the elements of this Act which affect Information Governance and data sharing and the disclosure of information to improve public service delivery. It states that three conditions must be met. A specified person may disclose information to another for the purposes of a jointly held objective. Schedule 4 of the Act describes who a 'specified person' is and includes:

- Central Government Departments
- Local Authorities, including County and district councils, Fire and Police
- Schools and Academies
- Gas and electric Markets Authority
- Chief Land Registry
- A person providing services to a Local Authority .
-

The objective must comply with these conditions:

1. The first condition is the improvement or targeting of a public service provided to individuals or households, or the facilitation of the provision of a benefit (whether or not financial) to individuals or households.

2. The second condition is that the objective has as its purpose the improvement of t he well-being of individuals or households.

Well-being meaning:

- their physical and mental health and emotional well-being,
- the contribution made by them to society, and
- their social and economic well-being.

3. The third condition is that the objective has as its purpose the supporting of the delivery of a specified person's functions, or the administration, monitoring or enforcement of a specified person's functions.

Code of Practice covering Part 5 of the Act

http://www.legislation.gov.uk/ukpga/2017/30/part/5/enacted

Part 5 of the Digital Economy Act 2017 introduces a number of new powers to share information to help make the digital delivery of government services more efficient and effective. Sections 35 to 39 (public service delivery), section 48 (debt owed to the public sector) and section 56 (fraud against the public sector) create specific gateways to share information for the purpose of improving public service delivery, and managing debt and fraud against the public sector respectively.

The Freedom of Information Act 2000

Section 1 – General right of access to information held by public authorities
http://www.legislation.gov.uk/ukpga/2000/36/section/1

Section 19 – Publication schemes
http://www.legislation.gov.uk/ukpga/2000/36/section/19

The Freedom of Information Act 2000 gives the public a general right of access to information held by public authorities. The Act also requires public authorities to have an approved publication scheme, which is a means of providing access to information which an authority proactively publishes.

When responding to requests, there are procedural requirements set out in the Act which an authority must follow. There are also valid reasons for withholding information, which are known as exemptions from the right to know.
It is considered good practice to include information relating to information sharing on the publication scheme in each relevant authority. This does not mean that the information shared should necessarily be included but the reasons why information is being shared, which organisations are involved and the standards and safeguards that are in place.

The Local Government Act 1972

Section 111 – Subsidiary powers of local authorities
http://www.legislation.gov.uk/ukpga/1972/70/section/111

Section 111 of the Act enables an authority to do anything which is intended to facilitate, or is conducive or incidental to, the discharge of any of its functions, providing that it has the specific statutory authority to carry out those functions in the first place.

Localism Act 2011

Section 1 – Local authority's general power of competence
http://www.legislation.gov.uk/ukpga/2011/20/section/1/enacted

The general power of competence provides a new power available to local authorities allowing them to do "anything that individuals generally may do". There are conditions placed on the use of the Act in circumstances where what the Local Authority wants to do is prohibited by another statute.
The Information Commissioners Office has indicated that the legislation can be used as a basis to share information to identify and work with individuals and families to improve service provision and provide a more holistic approach to social care.

The Children Act 1989

Sections 17 – Provision of services for children in need, their families and others
http://www.legislation.gov.uk/ukpga/1989/41/section/17
Section 27 – Co-operation between authorities
http://www.legislation.gov.uk/ukpga/1989/41/section/27
Section 47 – Local authority's duty to investigate
http://www.legislation.gov.uk/ukpga/1989/41/section/47
Schedule 2 – Local authority support for children and families
http://www.legislation.gov.uk/ukpga/1989/41/schedule/2

Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm.

It states that unless in all the circumstances it would be unreasonable for them to do so, the following listed authorities must assist a local authority with these enquiries if requested, in particular by providing relevant information.

- local authority;
- local education authority;
- housing authority;

- health authority;
- person authorised by the Secretary of State.

A local authority may also request help from those listed above in connection with its functions under Part 3 of the Act. Part 3 of the Act, which comprises of Sections 17-30, allows for local authorities to provide various types of support for children and families.

Section 17 places a general duty on local authorities to provide services for children in need in their area.

Section 27 enables the authority to request the help of one of those listed above where it appears that such an authority could, by taking any specified action, help in the exercise of any of their functions under Part 3 of the Act. Authorities are required to co-operate with a request for help so far as it is compatible with their own statutory duties and does not unduly prejudice the discharge of any of their functions.

In practice, when required to help under Sections 47 or 17 of the Act, authorities may be approached by social services and asked to:

- provide information about a child, young person or their family where there are concerns about a child's well-being, or to contribute to an assessment under Section 17 or a child protection enquiry;
- undertake specific types of assessments as part of a core assessment or to provide a service for a child in need;
- provide a report and attend a child protection case conference.

The Act does not require information to be shared in breach of confidence, but an authority should not refuse a request without considering the relative risks of sharing information, if necessary without consent, against the potential risk to a child if information is not shared.

The Children Act 2004

Section 10 – Co-operation to improve well-being
http://www.legislation.gov.uk/ukpga/2004/31/section/10

Section 11 – Arrangements to safeguard and promote welfare
http://www.legislation.gov.uk/ukpga/2004/31/section/11

Section 10 places a duty on children's services authorities to promote co-operation between itself, its partners and other appropriate bodies carrying out functions in relation to children in the area in order to; improve physical and mental health and emotional well-being; provide protection from harm and neglect; provide education, training and recreation, promote their contribution to society; and social and economic well-being.

Section 11 places a duty on all relevant authorities to make arrangements to ensure that their functions are carried out with regard to the need to safeguard and promote the welfare of children.

An authority and its partners must have regard to any guidance issued to them by the Secretary of State when exercising their functions under this Section 10 and 11.

In order to safeguard and promote the welfare of children, arrangements should ensure that:

- all staff in contact with children understand what to do and are aware of the most effective ways of sharing information if they believe a child and family may require targeted or specialist services in order to achieve their optimal outcomes;
- all staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including those children suffering or at risk of significant harm.