DATA PROTECTION

POLICY AND PROCEDURES

Version 8 May 2019
This policy is also available in the Welsh Language.

Contents

FORWARD BY THE CHIEF EXECUTIVE

In delivering its services Denbighshire County Council will need to collect and process certain types of information about people including customers, service users, staff of the Council, school pupils and suppliers or providers of services to it. All such processing is subject to the General Data Protection Regulation and the Data Protection Act 2018. This published policy sets out the Council's intentions in fulfilling its' obligations.

Transformational and shared services agendas have introduced ever increasing requirements for the sharing of personal data in order to improve effectiveness and efficiency. Clearly those in public services need to keep this information secure, but it goes much wider than appropriate security and requires a comprehensive approach to the collection, use, sharing and retention of personal information, in order to build public confidence. Combined with the reliance on fast changing ICT capabilities and storage of vast amounts of data, it is essential that Denbighshire County Council has this overarching document in plain language, which makes clear the Council's approach to data protection and data sharing; and explains the rights of the individual in relation to the information we hold about them. Publishing a clear and explicit policy and having the right approach to raising awareness and skills of staff as they handle personal information, will be regarded as an integral element in promoting public trust in the way this Council handles the personal data entrusted to it.

We have all been made aware of high profile data breaches, and many officers who handle sensitive personal data will be aware of the Information Commissioner's powers to fine authorities up to the equivalent of 20 million euros for severe breaches. Many of the reported breaches are however simply down to human error, such as inputting the incorrect fax number, emailing the wrong recipient or not checking personal data before it is posted, leaving sensitive documents in the car or not checking a person's identity over the phone. These errors can all be avoided by officers and members taking extra care in going about their duties and treating others' personal information, as they would their own.

The Council signed up to the Wales Accord on the Sharing of Personal Information (WASPI) in 2011, which applies to data sharing across multiple agencies in Wales. This national policy approach will be ever more important, as we continue to collaborate in order to deliver joined up public services within resources.

I am pleased to support the 'Personal Information Promise' set out overleaf. It is a form of mission statement, for the handling of personal information aimed at those whose personal information we hold. If a compliance problem occurs we will reflect on whether we are living up to this promise, and I urge all staff to read this promise as it puts the Data Protection Act obligations into straightforward language that we can all understand and put into practice.

PERSONAL INFORMATION PROMISE

Denbighshire County Council promises that it will:

1. Value the personal information entrusted to us and make sure we respect that trust;

2. Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4. Be open with individuals about how we use their information and who we give it to;

5. Make it easy for individuals to access all their personal information;

6. Keep personal information to the minimum necessary and delete it when we no longer need it;

7. Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

8. Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;

9. Put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and

10. Regularly check that we are living up to our promises and report on how we are doing.

INTRODUCTION

Denbighshire County Council shall at all times comply with its duties under the Data Protection Act 2018 and the rights of privacy and respect for personal and family life set out in Article 8 of the Human Rights Act 1998.

The Data Protection Act 2018 (the Act) incorporates the General Data Protection Regulation (GDPR) and places legal obligations on organisations who collect and use personal information and gives individuals certain rights of access. In addition, there are stricter requirements in the Act in respect of processing 'special category data'. Personal information can be held in any format eg electronic, paper records, CCTV or photographic images and the Act applies irrespective of how the information is held.

RESPONSIBILITY FOR THE ACT

The Council is committed to ensuring all staff, including agency staff, elected members, volunteers, and contractors comply with the Act. The full Council has appointed a statutory Data Protection Officer (DPO) who is responsible for ensuring compliance with the Act, assisted by the Business Information Team and the Council's Access to Information Panel and the Information Governance Group. The Council's Head of Business Improvement and Modernisation is the appointed Senior Information Risk Officer. (SIRO) There is also a nominated Information Management Officer sitting within each service. The Council's Officer Scheme of Delegation sets out clearly that all Heads of Service are responsible for compliance with the Act, and the decisions of the Access to Information Panel regarding the release or withholding of information. All staff must undertake the Council's mandatory training on Data Protection.

There is a separate policy in respect of the Freedom of Information Act and the Environmental Information Regulations. Where a request is received under the FOIA or the EIRs but in fact it falls within the Data Protection regime, the Council will automatically channel it through the appropriate policy, as it is required to do, as different exemptions and therefore, different legal rights apply in the circumstances. In some circumstances, a request can fall into two or more of these regimes; in this situation some information may for example be withheld under one regime, but released under the other.

The public interest test, applicable to both data protection and freedom of information; will be a key component of our decision making, to enable the public and citizens receiving services, to have confidence that we are delivering our functions to the quality and standard required.

Denbighshire Schools have their own data protection policy, and any such request the Council receives for the schools' information may be referred to the relevant school for processing.

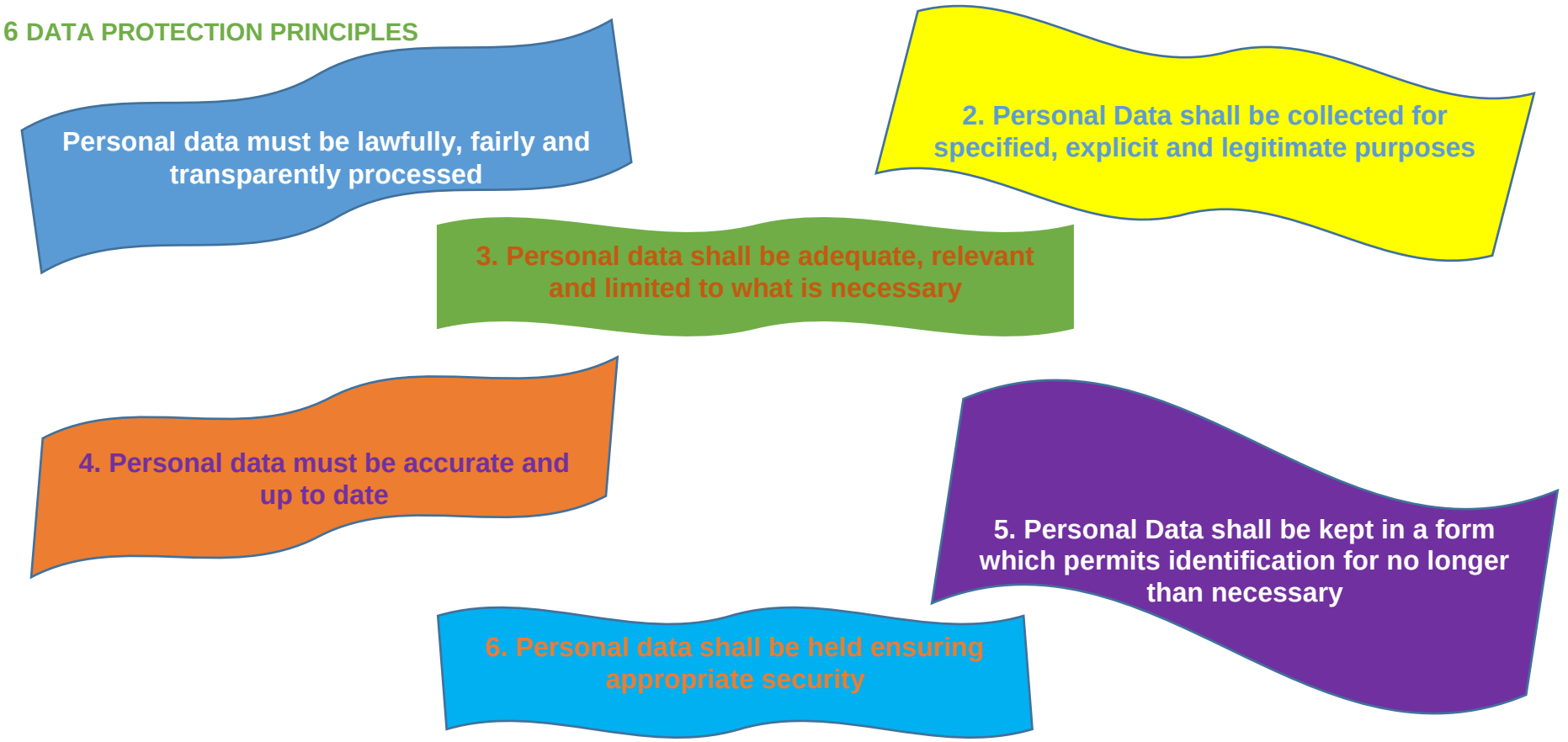
Elected members are data controllers in their own right in respect of processing in relation to their ward and constituents, however when they are processing Council information, the Council is the data controller. Councillors have the use of the Council's email system for both council and ward processing. Training is available on their obligations.

SCOPE

This policy applies to all personal information held in any recorded format such as handwritten notes, email, paper, video, CCTV or photographic images and applies to all officers, (including agency or temporary staff), volunteers and elected members, who process personal data on behalf of the council. It is a criminal offence to destroy personal information when the purpose of the destruction was to avoid disclosure following a request. It may also be a disciplinary offence to refuse to disclose information where the advice is that this information should be released.

ADHERING TO THE 6 PRINCIPLES OF THE ACT

The Data Protection regime is underpinned by 6 certain fundamental principles, which form a code for the proper processing of personal data. Processing means anything we do with data; such as obtaining, copying, disclosing, altering, retaining or destroying information. If we cannot comply with all these 6 principles, we should not be processing the data. The principles are summarised in the following diagram: -



The Council will ensure that: -

- It has in place procedures for complying with the six principles.

- All new staff receive appropriate data protection training on induction and that refresher training and guidance is provided periodically, so that they understand that they are contractually responsible for complying with the law and know how to process information in accordance with these 6 principles.

- Advanced level training is provided to those Officers who deal with highly sensitive personal information, such as social services. Training needs mapping will be conducted to identify those officers who require regular advanced training on data protection and information sharing, to enable them to share with confidence and in accordance with WASPI where appropriate.

- Everyone managing and handling personal information are individually and collectively responsible for compliance with this policy.

- A failure to follow this policy by an officer may result in disciplinary action or even criminal prosecution in the case of a wilful and deliberate breach.

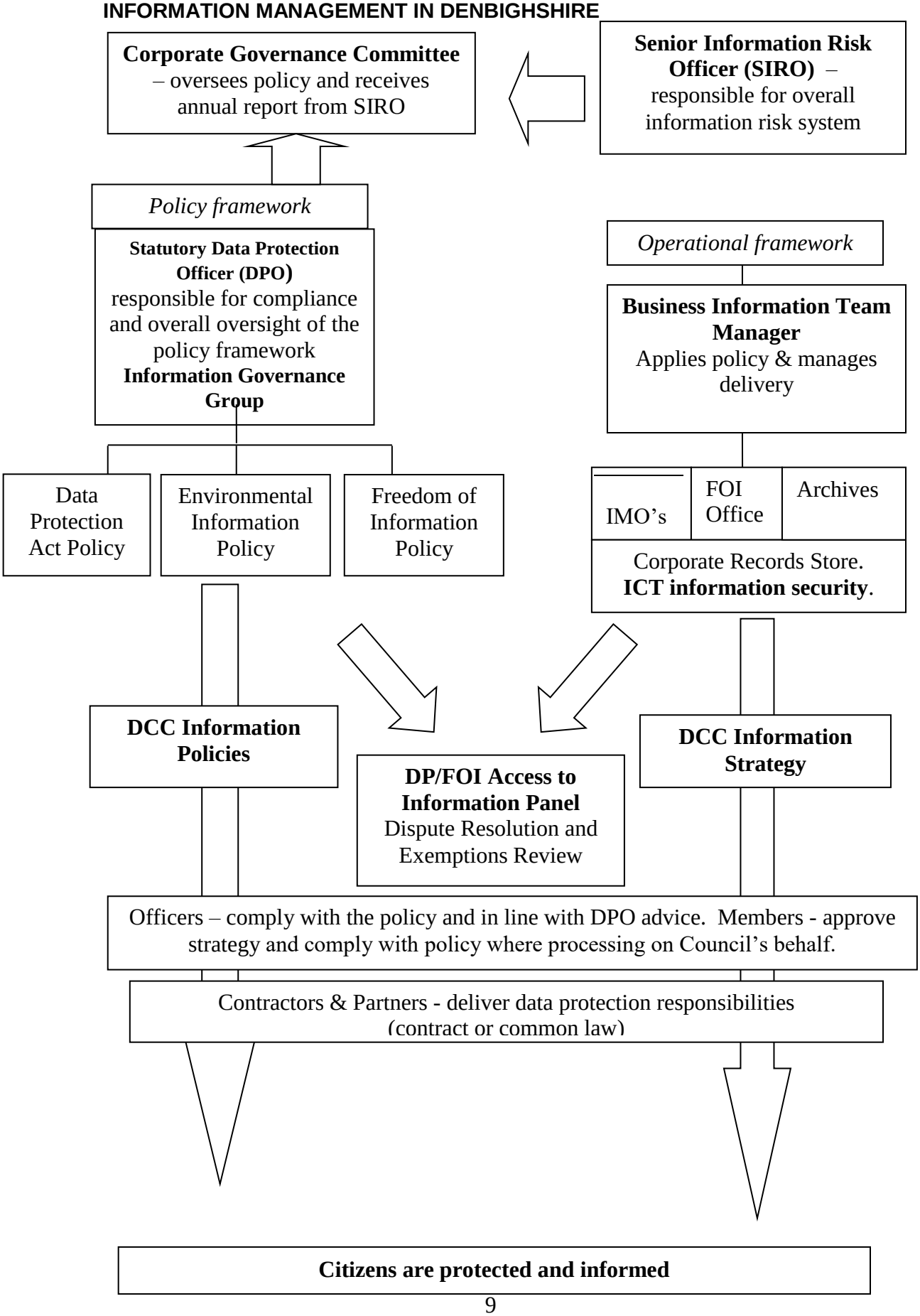
- That individuals are informed of the purposes for which their data will be used and the legal ground for processing the information is applied.

- All staff are trained to recognise a subject access request and what to do; including following specialist advice from the Council's Data Protection Officer.

- All appropriate, technical and organisational security measures to safeguard personal information will be put in place including encrypting or ensuring increased security settings of removable devices such as laptops or mobile phones and restricting the use of USB sticks in line with the Council's Information Security Policy.

- All staff are required to report data security incidents, including 'near misses' to their line manager who shall inform the DPO and the SIRO.

INFORMATION MANAGEMENT IN DENBIGHSHIRE



INDIVIDUAL'S RIGHTS

Denbighshire County Council will ensure that individuals can exercise their rights as set out in the Act including:-

- the right to be informed of the purposes of the processing;
- the categories of personal data being processed;
- the right of subject access to their personal information;
- who will or is likely to receive their information;
- the envisaged period for which the data will be stored;
- the right to prevent processing of personal information in certain circumstances;
- the right to rectify, block, erase, restrict, object or correct inaccurate information;
- the right to lodge a complaint;

These rights apply to all living, identifiable individuals on whom the Council processes personal information such as our customers, staff, residents, citizens receiving services or Councillors.

SUBJECT ACCESS REQUESTS

All requests for information should be sent to the Council's Business Information Team, this can be done in writing by post or online on the Councils' website, the request will be logged and referred to the relevant service to collate and retrieve. Citizens are able to make requests verbally, although the Council would encourage applicants to use the standard application form in order to assist officers in retrieving the correct information and to avoid any confusion.

The GPDR does not set out different procedures for social services or education for example; therefore the standard corporate procedures will apply to all services of the Council.

Article 15 of the GDPR provides the right for individuals to be told by the Data Controller (the organisation who determines the purposes for which and the manner in which personal information is processed).

- if we hold information about them,
- to ask what we use it for,
- to be given a copy of the information, whether council or third party information,
- to be given details of other organisations or people we disclose it to,
- to ask for incorrect data to be corrected,
- to ask us not to use personal information about them for direct marketing,
- to be compensated for damage or distress if we do not comply with the Act,

- to object to decisions made only by automatic means – for example where there is no human involvement,
- to ask the Information Commissioner's Office to investigate and assess whether we have breached the Act.

Denbighshire County Council will supply this information providing the request is made verbally or in writing; and sufficient information is given by the applicant to enable the Council to locate the information requested. All such requests, received from all services, must be logged with the Business Information Team who will oversee compliance within legal timeframes and advice on disclosure of subject access requests, with support from the DPO or legal services as required.

There is no fee applicable and the Council must respond within one month, unless the request is complex or multiple, in which case it may be extended by two further months. This one month time limit includes situations where third party comments are sought; the Council must still comply with these time limits, and where comments or consent are not forthcoming, then the law allows the Council to make a decision without such comments or consent. Access to ones' personal information is the cornerstone of the legislation, and this is likely to be of greater weight than third parties' views, unless there is a genuine legal reason to refuse.

Where the third party refuses consent, this in itself is not a reason for the Council to refuse to disclose the information. Neither should reliance on obtaining third party consent be a reason to delay processing the request. The decision on disclosure is one for the Council not the third party.

If the Council is extending the time frame to enable compliance with a subject access request, it shall write to the applicant advising of the circumstances, and setting out the reasons as to why.

The Council will respond to such requests within one month, unless the request is voluminous, manifestly unfounded or excessive. There is no definition within the Act, but in respect of an 'excessive' request, it is generally taken to mean that the effort the organisation would have to expend in complying with the requirement to provide a copy, is disproportionate to the benefit to be derived by the individual in receiving it. In such circumstances the Data Protection Officer will consider a refusal of the request and may refer the decision to refuse to the Access to Information Panel.

As the right of access to one's own information is fundamental to data protection law, the circumstances where disproportionate effort can be relied upon, will be rare. Advice should be sought from the Business Information Team and/or the DPO, in the first instance and a decision referred to the Access to Information Panel.

The Council will provide the information in a permanent format that is understandable to the applicant, unless the supply of such a copy would involve disproportionate effort, or the applicant agrees otherwise. The Council will where possible, encourage electronic secure transfer, as this is more secure and more economical to the public purse.

Fees

The GDPR only allows the Council to make an administrative charge for requests which are manifestly unfounded or excessive. The Council' policy is that it will refuse such requests and therefore there will be no requirement to raise a fee.

Currently there is no legal power allowing the Council to make any other charges; administrative or otherwise. This policy will be updated as and when any such Regulation is passed by Parliament. [1]

What about requests for information about children or young people under 18?[2]

All the rights set out in the paragraph above are equally applicable. However, it should be remembered that even if a child is too young to understand the implications of the subject access rights, it is still the right of the child rather than anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility.

Before responding to a subject access request for information held about a child, the Council should consider whether the child is mature enough to understand their rights. If the Council is confident that the child can understand their rights, it should respond directly to the child. The Council may however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the Council should take into account, (in no particular order) among other things:

- the childs' level of maturity and their ability to make decisions like this,
- the nature of the personal data,
- any court orders relating to parental access or responsibility that may apply,
- any duty of confidence owed to the child or young person,
- any consequences of allowing those with parental responsibility access to the child's or young persons' information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- any views of the child or young person has on whether their parents should have access to information about them.

In Scotland there is a presumption that a person 12 years and over is of sufficient age and maturity, unless the contrary is shown. The law in Wales does not specify an age and competence is assessed depending on the level of understanding of the child, but it does indicate an approach that will be reasonable.[3]

[1] Data Protection Act 2018 section 12 limits fees that may be charged by Controllers.
[2] Extracted from the ICO guide to the GDPR 22nd March 2018.
[3] The test on Gillick competency is also helpful in the context of data protection requests.

Exemptions
The Council may also under the Act and Article 15 GDPR refuse disclosure of data under the right of access provisions, where the serious harm test is met in respect of disclosure of education, health or social care data.

Reviews
Individuals may seek a review of a decision to withhold information and this can be done by contacting the Access to Information Officer.

INFORMATION SHARING

Information sharing is a complex area spanning many statutes and often the detail is hidden in secondary legislation (such as orders or statutory instruments). Decisions on whether to share information must be taken on a case-by-case basis and there could not be a blanket policy statement for officers or members to follow as this is likely to be unlawful. In addition, understanding what can legally constitute 'consent', is also fundamental.

However, the following statements should clarify previous common myths or misunderstandings regarding information sharing:

The Data Protection Act does not prevent, neither should it be seen as a barrier, to lawful information sharing.

The Council is not legally required to have an Information Sharing Protocol in place, in order to share. The lack of an ISP should not be a reason for not sharing information that could help a practitioner deliver services to a person.

The Council has signed up to the Wales Accord on the Sharing of Personal Information (WASPI), however not every information sharing arrangement will need to be WASPI approved.

Consent is not a prerequisite to information sharing – but several legal regimes (including the Data Protection Act) confirm that the obtaining of valid consent will permit information to be shared lawfully.

Confidentiality you may owe to an individual, can, and in some circumstances, must be overridden, such as concerns that a vulnerable adult or child may be at risk of serious or significant harm. Follow the relevant procedures without delay.

Over the page are seven golden rules for information sharing reproduced from the HM Government publication 'Information Sharing; Guidance for practitioners and managers' and available on the Department for Education website. These rules compliment the WASPI principles that the council has signed up to.

SEVEN GOLDEN RULES
for information sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately

2. **Be open and honest** with the person (and/or their family where appropriate) 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. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Requests from third parties (eg the Police) for an individual's personal information

Occasionally the Council may receive formal requests under the Act from other agencies or third parties such as the police, DWP or HMRC, solicitor's firms etc, to physically access or receive a copy of the information relating to an individual. These sections do not provide the Council with an automatic reason to disclose to these agencies, as is explained below.

The Act deals with several situations in which personal data is processed for the following 'crime and taxation' purposes:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and

- the assessment or collection of tax or duty.

The personal data could be disclosed if the disclosure is for any of the above crime or taxation purposes and the above purposes are 'likely to be prejudiced' if the Council did not disclose eg to the police or the inland revenue. The threshold for disclosure in these circumstances needs to be more than a mere risk of prejudice and needs to be a significant and weighty chance of prejudice to the above purposes. In such circumstances you would need the third party to set out what information they wanted to see (or envisaged) and what legal powers they are relying on and evidence of identity. Seek advice from the Business Information Team or the Data Protection Officer.

Disclosure of personal information over the telephone or face to face without establishing the identity of the recipient should be avoided.

Applications that are made by the police should be on the standard police form [insert name/no] which must be signed off by a police officer of the rank of Sergeant or above. If the application is not received in this way, fully completed then it should be referred back to the applicant. It is essential that we have a full audit trail with reasons why the police consider the necessity test applies.

Elected Members requests for information
The Act allows disclosures of personal information directly to elected members under Schedule 1 Part 2 paragraphs 23 and 24 without insisting on the written consent of a citizen, where the Member is acting with authority, in connection with the discharge of their elected representative functions and in response to a request by an individual that the elected representative take action on their behalf. A guidance note is available from legal services on request.

CCTV FOOTAGE

Denbighshire County Council's corporate public space CCTV system is currently managed by an external provider and all requests for such footage from members of the public should be made to the Business Information Team, who shall liaise with the provider. CCTV footage is subject to the CCTV Code of Practice, the Data Protection Act 2018, and the Regulation of Investigatory Powers Act 2000 in respect of where its use is deployed as part of covert surveillance. The Council is the Data Controller for such information.

Denbighshire County Council also utilises overt internal and external CCTV cameras situated in and on municipal and certain residential premises (such as care homes) in order to protect and prevent crime, monitor visitors (including staff) improve security and health and safety arrangements. All staff shall comply with this Data Protection Policy whilst carrying out their duties, and a breach may result in disciplinary action.

Where CCTV forms part of a Subject Access Request applicants will need to be very specific about the time and locality of their placement as otherwise the Council will not be able to deal with the request.

Individual services, such as parking services, may also wear body footage cameras that do not form part of the corporately outsourced system but must still comply with this Data Protection Policy.

Any CCTV system must be compliant with the 12 guiding principles of the Surveillance Camera Commissioner's Code of Practice June 2018 or as amended.

OCCUPATIONAL HEALTH INFORMATION

The majority of staff' personal information processed by the Occupational Health Unit will be held under the Data Protection Act 2018 and the Access to Health Records Act 1990.

EMERGENCY PLANNING

The guidance given on pages 10 and 11 on information sharing are equally applicable in the context of emergency planning and dealing with the provision of vital services in response to an emergency. The Data Protection Act 2018 does not prevent information being shared, and complements the Civil Contingencies Act 2004 – officers who require more detailed guidance (albeit refers to the DPA 1998 not 2018) may wish to consult the HM Government publication 'Data Protection and Sharing' – Guidance for Emergency Planners and Responders and take advice, if needed, from legal colleagues.

> "The Data Protection Act 1998 is an important piece of legislation giving confidence to individuals that their personal data will be treated appropriately and that it will not be misused. It's job is to balance individuals' rights to privacy with legitimate and proportionate use of personal information by organisations. In the context of emergency planning – and, in particular, in the aftermath of an emergency – it is important to look at this balance critically and realistically. The public interest is highly likely to mandate the sharing of information to help both immediately affected individuals and the wider community in such circumstances. Indeed, our view is that emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information. We must all work within the law, but in the circumstances set out in this guidance, we feel that uncertainty should not be used as an excuse for inaction when it is clearly in the interest of individuals and the public at large to act positively"
>
> Forward by Baroness Ashton in HM Government's non statutory guidance 'Data Protection and Sharing' – Guidance for Emergency Planners and Responders.

Denbighshire County Council will adhere to this policy and have in mind the following broad brush, straightforward questions whilst planning and responding to an emergency. The following questions must be considered by officers in good faith and if so, they should have comfort that they have not breached the Act:

- Is it unfair to the individual to disclose their information?
- What expectations would they have in the emergency at hand?
- Is the Council acting for their benefit and is it in the public interest to share this information?

Following these broad principles in an emergency will mean the Council is very unlikely to have acted unlawfully.

OUTSOURCING PERSONAL DATA PROCESSING

What about our external suppliers and the Council outsourcing personal data processing?

The Council frequently uses third party organisations to perform some of it's functions. Where such 'outsourcing' arrangements involve the processing of personal data, certain legal obligations arise. These obligations are more onerous now under GDPR than under the old data protection legislation therefore extra care needs to be taken when entrusting a third party supplier with personal data. Seek advice if you are in doubt. Follow the Council's Contract Procedure Rules which are in the Constitution.

It is important that the obligations imposed on the supplier should be set out in a written contract or letter. If the Council's Standard Corporate Terms and Conditions have been used – these are available from the Procurement Unit – then the obligations are already set out.

In any event, where sensitive 'special category' personal information is being disclosed to such third party organisations, services should ensure that the council's standard terms of business are signed up to by the contractor, in order to ensure the supplier is contractually bound by the same obligations as ourselves.

Care also needs to be taken where the supplier could also be a joint Data Controller (rather than a data processor) and the contract terms and conditions should reflect these obligations so that the supplier is held legally responsible for breaches where appropriate. Seek advice from Legal Services on the appropriate contract terms.

Introduction of new systems that affect personal information – what should the Council consider?

In developing information systems or new business processes or changes to our existing processes, that involve personal information, it is now a requirement to carry out a Data Protection Impact Assessment (DPIA) and to build in privacy-friendly solutions as part of modernising or introducing new systems. This is referred to under the GDPR as 'Privacy by Design and Default' and the DPIA can be a useful tool to help identify risks and help the Council manage those risks and where possible eliminate them.

The Council has standard templates for carrying out DPIAs so you have an audit trail of how you have considered the impact of the new system on people's personal data. These are available to Council staff on the Business Improvement and Modernisation section of the intranet. Guidance can be sought from this team on their completion.

PRIVACY NOTICES

There is a legal requirement to provide individuals with a privacy notice at the point of collection of personal information. The Business Information Team can provide examples, where the corporate website notice may not be sufficiently detailed.

EMAIL USE AND DATA PROTECTION

Council staff should only use an authorised DCC email account to communicate in respect of Council business and functions. Under no circumstances should staff (including fixed term, temporary, supply, agency or otherwise) use their personal email account to communicate personal information; in order to protect all individuals concerned. In addition, staff shall not send council personal data to their own personal email address without authority and a business reason to do so. Any staff member communicating or transmitting data in breach of this policy may face disciplinary action, and place the Council in the position of self-reporting such breaches to the ICO.

Highly sensitive information should be communicated via a secure email service such as egress, or approved governmental secure email system such as TLS (Transport Layer Security).

The Council's Information Security Policy will also apply to the use of email.

INFORMATION ASSET REGISTER

Services must keep their section of the corporate 'Information Asset Register' fully up to date. It is a legal requirement under GDPR for the Council to maintain such a register, which should be reviewed periodically by services. The Council is obliged to self assess its compliance levels and can only do this if it knows what data it holds, where it is, how it is held, how long its' retained, to whom is it disclosed and the lawfulness or powers to process in the first place. Any new processing or new systems or additional data collected, services should be considering if the Information Asset Register needs to be updated to reflect this change, together with consideration of completing a DPIA.

This Register is available to Council staff under 'Apps' on the Council's intranet.

CORPORATE RETENTION SCHEDULE

This is readily available to Council staff under 'Apps' on the Council's intranet and sets out the required retention periods for the Council's personal and non-personal information.

DATA SECURITY BREACHES

All data security breaches, including 'near misses', must be reported to the Line Manager responsible for the information in the relevant service who shall immediately inform the Council's Senior Information Risk Officer via email to dataprotection@denbighshire.gov.uk who shall advise on the necessary steps that need to be taken to contain any resultant damage, recover any lost information if possible, and inform individuals who may be affected. The Council has a breach procedure that it will follow. A central record of all breaches will be retained by this senior officer. The Council must inform the ICO of serious breaches within 72 hours.

OVERSIGHT ARRANGEMENTS AND REVIEW OF POLICY

This policy will be reviewed no later than January 2025. Compliance with this policy and related procedures will be monitored by the Data Protection Officer and the Business Information Team working with the Information Management Officers from each service, and the Councils Information Governance Group. Reports by the Business Information Team and the Councils activities under all the Information Legislation are reported annually to the Council's Corporate Governance Committee whereby the Senior Information Risk Officer and the Data Protection Officer shall be in attendance.

COMPLAINTS

A review of the Council's decision to *withhold* personal information where an applicant has made a subject access request, can be made to the Information Unit who will facilitate a review by the Access to Information Panel. If the decision is upheld, and the applicant remains unsatisfied they may appeal to the Information Commissioner's Office. Appeals against the decision of the Information Commissioner can be made to the Information Tribunal.

Any complaints by individuals about the way in which the Council has *handled* personal information (eg if it has lost personal information) will be dealt with through the 'Your Voice' Corporate Complaints or Social Services Complaints Policy depending on the nature of the information. Complaints forms are available from the Council's Offices. If the complainant remains dissatisfied, a complaint can be made directly to the Ombudsman's office.

CONTACT DETAILS

Access to Information Officer
Denbighshire County Council
County Hall
Wynnstay Road
Ruthin
Denbighshire
LL15 1YN
Email: information@denbighshire.gov.uk

Your Voice,
Denbighshire County Council
P O Box 62
Ruthin
LL15 9AZ

Tel: 01824 706000
Online: www.denbighshire.gov.uk and follow the links to the online form 'Suggestions, compliments and complaints'

Or in person you can tell a member of staff at a One Stop Shop

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel 01625 545745
www.informationcommissioner.gov.uk

Wales Accord on the Sharing of Personal Information
The WASPI team is currently hosted by the health authority and their contact details and live ISP's are available on their website www.waspi.org

Denbighshire County Council Senior Information Risk Officer (SIRO)
Head of Business Improvement and Modernisation
Level 3
County Hall,
Wynnstay Road,
Ruthin,
Denbighshire
LL15 1YN
Tel: 01824 706000

Denbighshire County Council Data Protection Officer/
Deputy Monitoring Officer
Legal and Democratic Services
Level 2
County Hall
Wynnstay Road
Ruthin
Denbighshire
LL15 1YN
Tel: 01824 706000

APPENDIX: ACCESS TO INFORMATION PANEL

Terms of Reference

Panel members:

- Head of Legal, HR and Democratic Services
- 1 x Head of Service
- Senior Information Risk Officer
- Data Protection Officer
- Business Improvement Manager

The panel is quorate when at least any one member and one legally qualified member is in attendance; remote attendance is also permissible.

Role and purpose

The purpose of the Access to Information Panel is to reach decisions on the disclosure or withholding of information following the receipt of a request for information under the Information Legislation, including disclosures under the Data Protection Act. The purpose of the Panel is not to provide an additional layer of bureaucracy, but to ensure consistency of approach in all areas of disclosure across the Council, with the emphasis on open government and transparency, in order to increase public confidence in the Council's decision making but also its obligations to protect personal information. It will also provide Services with the option of a reference to the Panel where they consider an exemption is applicable, against the views of the Business Information Team.

The Panel will make decisions on the following:

- Contentious, highly sensitive or very high profile exemption decisions.
- Requests for a review of an initial decision where the DPO or SIRO consider it appropriate for a reference to this panel.
- References from a Service who specifically wish the matter to be decided by the Panel.

The Panel will not make decisions on the following:

- Straightforward third party redactions of personal information.
- Exemptions which in the view of either the Head of Legal and Democratic Service, the Data Protection Officer, the SIRO or the Business Information Team are clearly applicable to the request and will not require the resources of a panel meeting.

.

Terms of membership

It is a condition of the panel membership that all panel members attend training on the Information Legislation in order to understand and apply the exemptions properly.

A full panel member cannot delegate its responsibility to another Officer who is not a panel member.

Where a conflict of interest affects a panel member's decision making, they must advise the panel of this interest and not take part in the decision. They may take their 'hat' off as panel member and make representations from their Service, but they cannot vote on the issue.

Panel members shall keep confidential the personal details of the requestor and any confidential information they are privy to, in their capacity as panel members.

Quorum

The Panel shall only be quorate when at least one legally qualified officer is present and at least one other panel member.

Wherever possible the Panel shall endeavour to reach a unanimous decision. Where this is not achieved, each member shall have one vote. Any matter will be decided by a simple majority of those members voting and present.

Process and Procedures

A referral to the Access to Information Panel shall be through the Business Information Team, who will then make arrangements for the Panel to meet, taking into consideration the statutory time limits in which the Service needs to deal with the request.

The department wishing to rely on the exemption may be invited to attend the panel, but their attendance is not mandatory.

The Access to Information Panel members shall use their best endeavors to attend any urgent meetings where this is necessary and unavoidable; however reasonable notice must be given to Panel members. If appropriate, urgent decisions may be made electronically, providing the request is not complex or necessitates the personal attendance of the department wishing to rely on the exemption.

s.36 Freedom of Information exemptions.

The Head of Legal, HR and Democratic Services is the sole panel member for s.36 decisions, who shall consult and itemize the issue before the panel, and take the panels' views, and any other relevant person, into consideration, prior to a final decision under this section.