CYNGOR
Sir Ddinbych
Denbighshire
COUNTY COUNCIL

DATA PROTECTION

POLICY AND PROCEDURES

Version 4 – April 2013

Foreword 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 Data Protection Act and this 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 to the public 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 £500,000 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. A number of underlying WASPI protocols have since been developed with our partners. In addition, in respect of any data processing generally, I am pleased to sign off the 'Personal Information Promise' set out overleaf, which will be registered with the Information Commissioner – 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

I, Mohammed Mehmet, Chief Executive, on behalf of Denbighshire County Council promise that we 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 and correct 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.

Signed:

Dated:

Introduction

Denbighshire County Council shall at all times comply with its duties under the Data Protection Act 1998 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 (the Act) 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 'sensitive' personal 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 comply with the Act. The Council has an appointed Data Protection Officer who is responsible for ensuring compliance with the Act, assisted by the Information Unit and the Councils Access to Information Panel. The Head of Business Planning & Performance is the appointed Senior Information Risk Officer. (SIRO) There is also a nominated Information Management Officer within each department. 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.

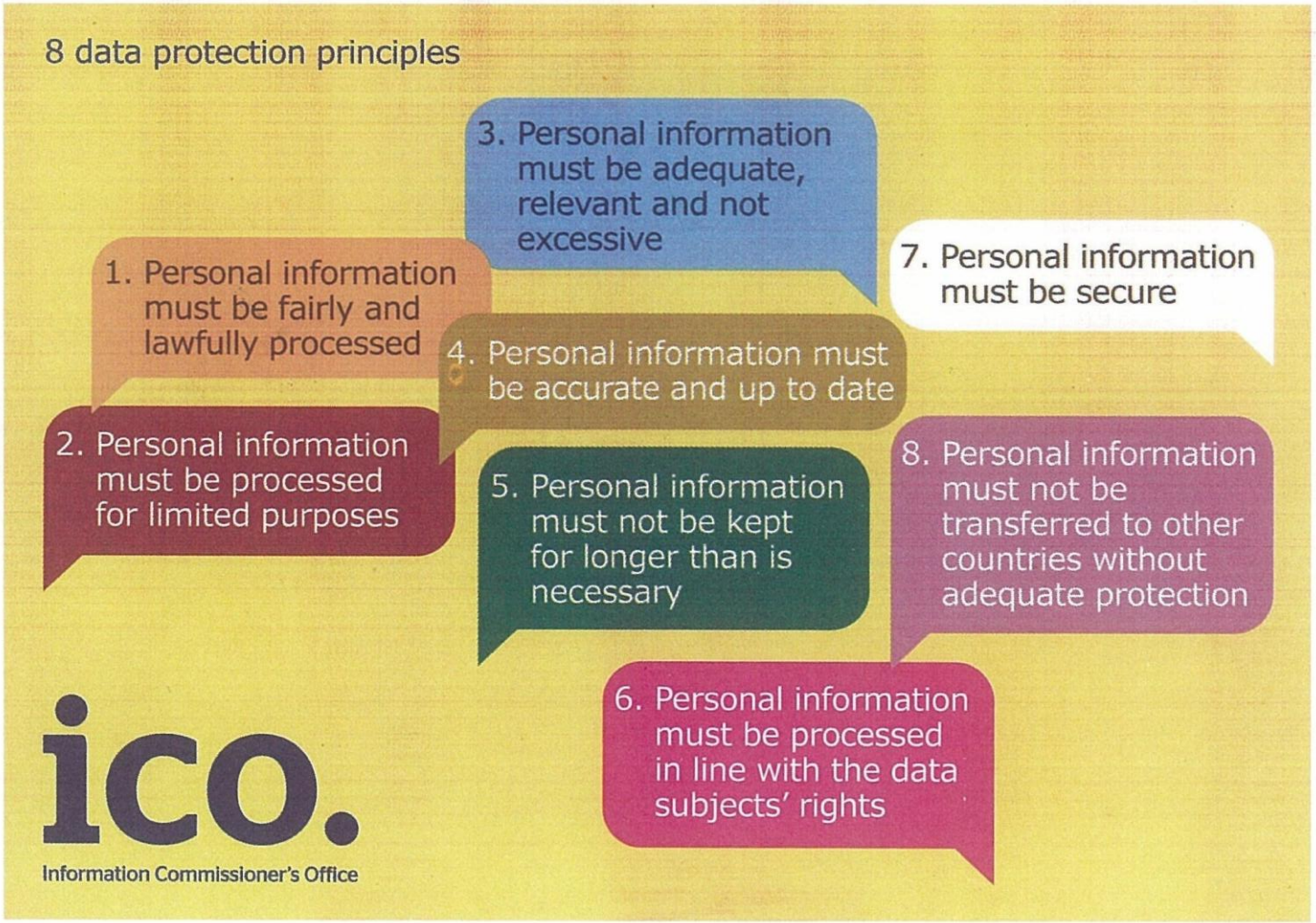
There is a separate policy in respect of the Freedom of Information Act and the Environmental Information Regulations. Where a request is received under the FOIA or the EIRs but in fact it falls within the Data Protection regime, the Council will automatically channel it through the appropriate policy, as it is required to do, as different exemptions and therefore, different legal rights apply in the circumstances.

Scope

This policy applies to all personal information held in any recorded format such as email, paper, video, CCTV or photographic images and applies to all officers and 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.

Adhering to the 8 principles of the Act

The Data Protection regime is underpinned by 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 8 principles, we should not be processing the data. The principles are reproduced as set out in the legislation at Appendix 1, but are summarised in the following diagram: -


8 data protection principles
1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection
ico.
Information Commissioner's Office

The Council will ensure that: -

- It has in place procedures for complying with the eight 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 8 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 by the Information Unit, in conjunction with Service and Performance Managers 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.

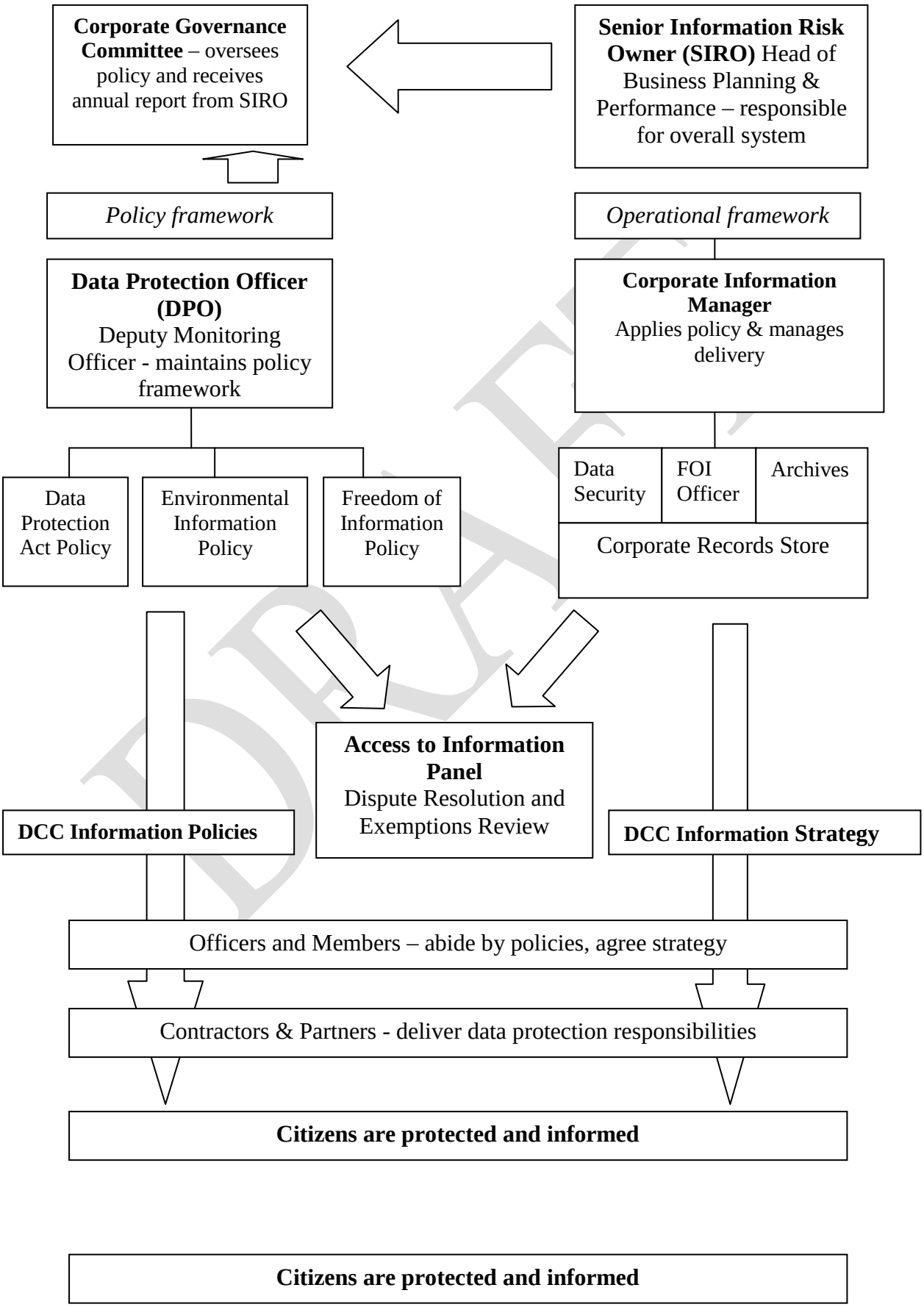
- A failure to follow this policy by an officer may result in disciplinary action or even criminal prosecution in the case of a wilful and deliberate breach.

- That individuals are informed of the purposes for which their data will be used and that consent is sought for such use, where required under the Act.

- 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 SIRO.

Information Management in Denbighshire



Citizens are protected and informed

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 that processing is being undertaken,
- the right of subject access to their personal information;
- the right to prevent processing of personal information in certain circumstances
- the right to rectify, block, erase or destroy inaccurate information.

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

Subject Access Requests

Section 7 of the Act 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,
- 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 and
- 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 in writing; sufficient information is given by the applicant to enable the Council to locate the information requested and a maximum

statutory fee of £10 is paid by the person making the enquiry in advance. All such requests must be logged with the corporate Information Unit. This fee may be waived in respect of social services customers accessing their social services records or employees of the Council who are accessing their personnel file.

Denbighshire County Council will respond to such requests within 40 calendar days of receipt, unless to do so would involve 'disproportionate effort' under Section 8 of the Act. There is no definition within the Act, but 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. As the right of access to ones 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 Information Unit 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. Where this is the case, the Council will arrange for the applicant to inspect the records in person.

Social Services Records

Social Services have their own procedures for dealing with client access to personal files, in accordance with guidance issued by the National Assembly of Wales and if necessary can offer support, guidance or even counselling to service users where this is required whilst they inspect their records. If the client makes the request under Section 7 of the Act, this still needs to be logged with the Information Unit who will record the details of the request itself.

In accessing their file, social services clients *may* not be given access to parts of their file which also identify other people without that third party's agreement, even if they are related. Disclosure will depend on the context and whether information is already within knowledge. Seek advice if in doubt. Information provided to social services by another person (except a professional such as a social worker or doctor etc) if this was communicated in confidence, information which may be seriously harmful to the individual or others, or information held to detect crime or to prosecute offenders where its disclosure will affect these purposes; may be lawfully refused. Legal advice should be sought if there is any doubt regarding the disclosure and a reference to the Access to Information Panel may need to be made.

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 will receive requests under the Act under s.29 or s.35 from other agencies or third parties such as the police, DWP or another Council, under these sections, 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, as is explained below.

s.29 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. s.29 is a *discretionary* power, and does not of itself give the Council a reason to disclose in itself as the Council still needs a Schedule 2 (and Schedule 3 reason in respect of sensitive personal data) to disclose.

s.35 also provides a *discretionary* power to disclose only where the disclosure is necessary 'for or in connection with legal proceedings (including prospective proceedings); for obtaining legal advice or for establishing, exercising or defending legal rights. The mere fact this exemption may apply does not, of itself, provide the Council with justification to hand over personal data. The Council will still need a Schedule 2 reason in order to do so (and a Schedule 3 reason in the case of sensitive personal data). Even then, there may be a legitimate reason not to disclose if the information is private and confidential or because of the relationship the Council has with the individual.

The Council's usual standard approach in respect of applications under s.29 and s.35 will be to refuse disclosure unless the applicant obtains a court order; however if the department or service consider that disclosure is in fact necessary or may very well prejudice the crime or taxation purposes, then advice should be obtained prior to disclosure from Legal Services and guidance on whether the decision on disclosure should be referred to the Council's Access to Information Panel.

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.

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 1998 does not prevent information being shared, and complements the Civil Contingencies Act 2004 – officers who require more detailed guidance 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"

Foreword 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

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.

It is important that the obligations imposed on the supplier (known as the data processor) 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 the event that the standard terms of business have not been, or are not used, the service should be asking the supplier to sign a letter, a template is attached as Appendix 3.

In any event, where sensitive 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.

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, Officers are strongly advised to consider the benefits of a Privacy Impact Assessment and to build in privacy-friendly solutions as part of modernising or introducing new systems. This is referred to by information professionals as 'Privacy by Design' and can be a useful tool to help identify risks and help the Council step up to the mark in how it handles personal information confidently.

Denbighshire County Council's Corporate Project Methodology now requires the Council to consider whether a Privacy Impact Assessment should be conducted in the early stages of a project and support is available for this via the Corporate Information Unit in conjunction with Legal Services if required. Even where the formal project methodology is not followed designing in privacy protections and data protection compliance will need to be addressed.

Data Protection or Privacy Notices

Consent from the individual who is the subject of the data, is one condition that can legitimise the processing of personal data. In respect of 'sensitive' personal data, this consent needs to be express and not implied, if consent is relied upon. The Council may find the use in many circumstances where reliance on consent is used to provide the individual with a 'Data Protection Notice' (or sometimes referred to as a Privacy Notice or Statement'). This can be communicated verbally and verbal consent can be relied upon, although a signed form or some form of positive action such as accepting terms electronically by ticking a consent box, will be the most practical and reliable method. Customer Services for example at the first point of contact by telephone will give enquirers a verbal standard notice. Examples of Data Protection Notices, which will assist in complying with the First Data Protection Principle of fairness and the Second Principle of purpose, is set out below which can be adapted by a service to suit their specific needs. The basic legal requirement is that an individual is given at the point of collection, or as soon as possible after, a description of the Council's use of individual personal information. Further guidance is available if required from the Corporate Information Unit.

Eg Online Library :

I UNDERSTAND that the information I have provided will be processed by Denbighshire County Council for the purpose of its online library catalogue and the monitoring and management of this service. I understand that the personal information I provide will be stored and processed in accordance with the Data Protection Act 1998 and that no third party recipients will be provided with my personal data without my consent, unless required by law.

I understand that I have the right to request a copy of the personal data held about me and to correct any inaccuracies.

Eg School Transport collection of data

I UNDERSTAND that the information I have provided will be processed by Denbighshire County Council for the purpose of school transport provision, the monitoring and management of this service, including behavioural management and any anti social behaviour prevention programmes, fraud prevention and detection and any purpose related to this service provision. I understand that CCTV may be in use on some routes and that my child's footage and information will be stored and processed in accordance with the Data Protection Act 1998.

I CONSENT to the sharing of this information with other departments or Government Bodies and other organisations delivering a service that relates to the provision of school transport and its management and that they may contact me directly. I understand that I have the right to request a copy of the personal data held about me and my child and to correct any inaccuracies

Eg Verbal notice given by an Enforcement Officer wearing HeadCams:

"In order to comply with our data protection obligations I need to make you aware that this conversation and footage is being recorded by the body camera I am wearing. The information recorded, will be controlled and processed by Denbighshire County Council for the purpose of it's public protection and health and safety obligations to officers. The information that you provide will be retained only until any fixed penalty issued is discharged. You have the right to request a copy of the personal information held and to correct any inaccuracies. "

If a Service is developing a website and is collecting personal information then a privacy policy will be required. See the Councils Privacy Policy in respect of Meifod Wood Products at Appendix 4 as an example. Services will be encouraged to draft a policy along similar lines in advance of submitting the policy to the Corporate Information Unit for checking compliance.

Data Security Breaches

All data security breaches, including 'near misses', must be reported to the Line Manager responsible who shall immediately inform the Council's Senior Information Risk Officer who shall advise on the necessary steps that need to be taken to contain any resultant damage and inform individuals who may be affected. A central record of all breaches will be retained by this senior officer.

Oversight arrangements and review of policy

This policy will be reviewed no later than February 2016. Compliance with this policy and related procedures will be monitored by the Corporate Information Unit working with the Information Management Officers from each service and the Access to Information Panel. Reports on the Corporate Information Unit 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.

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 Information Commissioner. Appeals against the decision of the Information Commissioner can be made to the Information Tribunal.

Contact details

Corporate Information Unit
Denbighshire County Council
46 Clwyd Street
Ruthin
Denbighshire
LL15 1HP
Email: information@denbighshire.gov.uk
Tel no: 01824 707023

Your Voice,
Denbighshire County Council
County Hall
Wynnstay Road
Ruthin
Denbighshire
LL15 1YN
Tel: 01824 706075
SMS 07800140088
Email: your.voice@denbigshire.gov.uk
Online: www.denbighshire.gov.uk and follow the links to the online form 'Suggestions, compliments and complaints'

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
WASPI Support Team
Preswylfa
Hendy Road
Mold
CH7 1PZ
Tel: 01352 803398

Denbighshire County Council Senior Information Risk Officer (SIRO)
Head of Business Planning & Performance
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 706275

Appendix 1 – The 8 Data Protection Principles

1. **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –**

   (a) at least one of the conditions in Schedule 2 (of the Data Protection Act) is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (of the Data Protection Act) is also met.

2. **Personal data 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. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

4. **Personal data shall be accurate and, where necessary, kept up to date.**

5. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**

6. **Personal data shall be processed in accordance with the rights of data subjects under this Act.**

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

8. **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

Schedule 2

At least one of the following conditions must be met when processing personal data.

1. The data subject has given his/her consent to the processing.

2. The processing is necessary—

   (a) for the performance of a contract to which the data subject is a party, or

   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary—

   (a) for the administration of justice,

   (b) for the exercise of any functions conferred on any person by or under any enactment,

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) 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 are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

   (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3

At least one of the following conditions must be met when processing sensitive personal data in addition to meeting at least one condition from schedule 2.

1. The data subject has given his/her explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—

(a) in order to protect the vital interests of the data subject or another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—

(a) is carried out in the course of its legitimate activities by any body or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix 2

ACCESS TO INFORMATION PANEL

Terms of Reference

Denbighshire County Council is committed to compliance with all information legislation, the Human Rights Act and the common law duty of confidentiality. The Council approved the formulation of a corporate Access to Information Panel in April 2012 and the panel member's obligations and powers are set out in the officer Scheme of Delegation contained within the Council's Constitution and adopted by Full Council.

Panel members:

Full Members:

- Corporate Director: (Chair)
- Head of Legal and Democratic Services & Monitoring Officer (Vice Chair)
- Head of Business Planning and Performance/Senior Information Risk Officer
- 2 x Heads of Service

Advisory Members: .

- Corporate Information Manager
- Deputy Monitoring Officer/Data Protection Officer

The panel is quorate when at least one full member and one legally qualified member (who may be an advisory member) is in attendance.

The Archivist/Records Manager may deputise for the Corporate Information Manager.

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 Corporate 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 by a requestor.
- 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 the Head of Legal and Democratic Services or his deputy, and the Corporate Information Team are clearly applicable to the request and will not require the commitment and attendance of the panel.

.

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 full 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. In the event of an equilibrium the Chair shall have the casting vote.

Process and Procedures

A referral to the Access to Information Panel shall be through the Corporate 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.

Legal Services shall prepare the report for the panel outlining the issues, but the Panel shall be entitled to ask questions and consider factors outside of the report if they consider this relevant. Where recommended, Legal Services shall draft the response to the applicant. If due to shortness of time a written report is not available, legal advice may be given verbally at the Panel, and noted in the minutes.

The department wishing to rely on the exemption shall 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 Decisions

The Head of Legal 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 into consideration, prior to a final decision under this section.

Version 3 April 2013

Appendix 3

Dear Sirs,

Compliance with the Data Protection Act 1998
Title of Service to be provided: [ ]

As you will appreciate the Council needs to ensure it complies with its legal obligations under the Data Protection Act 1998 and in this regard we set out below the terms of the disclosure of personal data to you and our obligations to you under this arrangement. The law does not permit us to allow you to process such data unless we comply, and can demonstrate that we comply with certain requirements. This personal data will include [list the type of data to be disclosed] which we agree to disclose to you on the following terms.

1) Security

You and we will take appropriate technical and organizational measures against unlawful and unauthorized processing of the personal data and against accidental loss, destruction of and damage to the personal data. In particular, you and we are required to:

1.1 keep the personal data strictly private and confidential;
1.2 minimise disclosure of the personal data to third parties to the fullest extent possible;
1.3 allow access to the personal data strictly on a 'need to know' basis and use appropriate access controls to ensure this requirement is satisfied;
1.4 ensure that any recipients of the personal data are subject to a binding duty of confidentiality in relation to the data.

2) Personnel

You and we will take all reasonable steps to ensure the reliability of all personnel (whether employees or contractors) that may have access to the personal data and to ensure that they are adequately trained in the good handling of personal data.

3) Instructions

You will only act in accordance with our instructions which are to provide you with the [names and addresses /insert type of data]in order to [specify what they will do with the data]

4) Subcontractors

You and we are not permitted to subcontract any activity relating to this agreement that will involve a third party processing the personal data.

5) Transferring Data outside the EEA

You and we will not transfer the personal data to any territory outside the EEA without our prior written consent.

6) Retention of Personal Data

6.1 You and we will promptly amend or delete any personal data that you process for us for the purposes of this agreement.

6.2 You and we will retain the personal data only for as long as is necessary for the purposes of this agreement.

7) Ending this agreement

Either of us may end this agreement by giving [ ] days written notice to the other. When this arrangement ends you agree to destroy any personal data that we have disclosed for the purposes of this arrangement.

8) Law

This letter and the arrangement made under it will be governed by the law of England and Wales.

9) Third Party Rights

We agree that we enter into this arrangement for the benefit of ourselves and the individuals whose personal data you will process each of which will be entitled to enforce it. Other than that no other person shall be entitled to enforce it.

Please sign the enclosed copy of this letter to indicate your agreement to it's terms.

Yours faithfully

……..
Name
Job Title
For and on behalf of Denbighshire County Council

……
Name
Job Title/Authorised signatory
For and on behalf of [Insert supplier]

Appendix 4

Meifod Wood Products Privacy Policy

1. Introduction and General Terms

Meifod Wood Products is committed to protecting personal information when using this website. This privacy policy relates to our use of any personal information provided to us through this website. In order to provide you with the full range of services or products, we are sometimes required to collect information about you. This privacy policy explains the following:

- what information Meifod Wood Products may collect about you
- how Meifod Wood Products will use information we collect about you
- when Meifod Wood Products will use your details to contact you
- whether Meifod Wood Products will disclose your details to anyone else
- your choices regarding the personal information you have provided to us
- the use of cookies and how you can reject these cookies

As set out above Meifod Wood Products is committed to safeguarding your personal information. Whenever you provide such information, we are legally obliged to use your information in line with all laws concerning the protection of personal information, including the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003.

2. What information will Meifod Wood Products collect about me or my clients?

When you register with Meifod Wood Products to receive information or services or goods, we may ask for personal information about you or if you are registering on behalf of clients, about them. This can consist of information such as your name, email address, postal address, telephone or mobile number or date of birth. Different products or services we sell, may require different types of personal information, and in some circumstances, this may involve us holding sensitive personal data such as health and disability data. We will not ask you for information such as this unless this is necessary.

Cookies are used to store login information and order information. If you do not wish to use cookies you should disable them in your web browser. IP addresses are not collected.

3. **How will Meifod Wood Products use the information collected about you?**

Meifod Wood Products will use the information collected for a number of purposes including the following:

- 'service administration purposes' which means that Meifod Wood Products may contact you for reasons connected with your current or previous orders. Eg product recalls or to advise you that delivery may be delayed.
- 'electronic direct marketing' which means that we may contact you by email from time to time with details of any new products or services which may be relevant to you if you have used our services previously. This is known as 'soft opt in' and the Regulations referred to in part 1 above allow this in these circumstances. If you have not used us before, we will always obtain your consent, before sending direct marketing communications by email.
- 'direct marketing' we may send information to you in the post from time to time. If you do not wish us to do so please advise us.

4. **When will Meifod Wood Products contact me?**

We may contact you for the following purposes:

- in relation to any after sales service/care we provide.
- to invite you to participate in surveys about our services or goods
- for marketing purposes where you have specifically agreed to this.

5. **Will Meifod Wood Products share my personal information with anyone else?**

We will keep your personal information confidential except where its disclosure is required or permitted by law (for example to government bodies or law enforcement agencies) and generally we will only use your personal information within Meifod Wood Products and not share this personal information within Denbighshire County Council's other internal departments without consent.

6. **How long will Meifod Wood Products keep my personal information?**

We will hold your personal information on our system for as long as is necessary for the relevant service or as long as is relevant in any contract between ourselves and you. This time period will usually be in line with Denbighshire County Council's Corporate Retention Policy.

If you wish to have your details removed from our database, we will comply with your request eg to remove you from our electronic marketing database, but may need to keep your details for other purposes, depending on the reason why you provided us with that information. Eg should we need to recall a product you have purchased.

7. **Can I find out what personal information Meifod Wood Products holds about me?**

Under the Data Protection Act an individual has the right to request a copy of the personal information that Meifod Wood Products holds about them and to have any inaccuracies corrected. The Council charges £10 for such information requests as is permitted under the data protection law and will require you to prove your identity. This is in order to protect your information from disclosure to third parties without your consent. We will use reasonable efforts to supply, correct or delete personal information about you on our files. Please address such requests to our Data Protection/Freedom of Information Officer, Denbighshire County Council, The Old Gaol, 46 Clwyd Street, Ruthin, Denbighshire, LL15 1HP

If you have any comments about this privacy policy please contact the General Manager, Meifod Wood Products, Unit 4,. Colomendy Industrial Estate, Denbigh, Denbighshire, LL16 5TA or telephone 01745 816900 or via email at meifod.woodproducts@denbighshire.gov.uk