

PROVINCIAL GRAND LODGE OF EAST LANCASHIRE PROVINCIAL GRAND CHAPTER OF EAST LANCASHIRE

DATA PROTECTION ACT 1998

DATA PROTECTION POLICY

The Provincial Grand Lodge and the Provincial Grand Chapter of East Lancashire [the Province] are committed to ensuring compliance with the requirements of the Data Protection Act 1998 [the Act]. The Province recognises the importance of personal data and the importance of respecting the privacy rights of individuals. This Data Protection Policy [the Policy] sets out the principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

A paramount responsibility of all our employees and officers [the Designated Users] is to assist the Province to comply with this Policy. In order to assist compliance, we have produced This Data Protection Guidance document [the Guidance] which explains in more detail the requirements of the Act.

The Designated Users must familiarise themselves with both this Policy and the Guidance and apply the provisions of the Act in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal or removal from office.

Serious breaches could also result in personal criminal liability.

In addition, a failure to comply with this Policy could expose the Province to enforcement action by the Information Commissioner or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

For these reasons, it is important that all the Designated Users familiarise themselves with this Policy and Guidance in respect of the care necessary in the handling of personal data.

Provincial Grand Secretary / Scribe E
August 2008

The following outlines the various Data Protection principles and gives specific guidance to all the Designated Users.

Data Protection Principles

The Province, as the data controller, will comply with the following principles in respect of any personal data:

1. Personal data must be processed fairly and lawfully and must not be processed unless:
 - at least one of the conditions in Schedule 2 to the Act is met and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the Act is also met.

The Schedule 2 and 3 conditions are set out in the Guidance Section.

2. Personal data must be obtained only for one or more specified and lawful purposes and must not be further processed in any manner incompatible with those purposes.
3. Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data must be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data must be processed in accordance with the rights of data subjects under the Act.

These rights include

- subject access,
- the prevention of processing likely to cause damage or distress,
- the prevention of processing for purposes of direct marketing and
- objections to automated decision-taking.

The Province does not normally process data for the purposes of direct marketing or automated decision making.

7. Appropriate technical and organisational measures must 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 must 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.

This Policy may be amended from time to time to reflect any changes in legislation. Any queries / requests should be directed to the Provincial Grand Secretary.

DATA PROTECTION POLICY

GUIDANCE NOTES

INTRODUCTION

These Guidance Notes [the Guidance] form part of the Data Protection Policy and provides supplementary information to enable employees and officers to understand and comply with the Data Protection Policy.

The Province is required to comply with the Data Protection Act 1998 [the Act] in respect of its processing of personal data, particularly information concerning individual freemasons and employees. It is important for all Designated Users to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Act.

Failure to do so may expose the Province to enforcement action by the Information Commissioner and / or to complaints and / or claims for compensation from affected individuals. There may also be negative publicity as a result of a breach.

You are required to assist the Province in complying with its obligations under the Act. In order to do this, you must comply with the Data Protection Policy and this Guidance whenever you process personal data, as well as any other data protection related policy that may be applicable to your area of work.

Failure to comply with this policy could be a disciplinary offence, which might result in dismissal or removal from office.

Negligent or deliberate breaches could result in criminal liability for you personally or to action being taken under the masonic code of conduct.

Any questions concerning this policy should be raised with The Provincial Grand Secretary.

LEGAL FRAMEWORK

The Act sets out eight data protection principles, which must be followed in relation to all processing of personal data. These principles are set out in the Data Protection Policy and are reproduced below, together with an explanation of what they require.

The Province processes personal data. This includes a range of data subjects, particularly information concerning individual freemasons and, also, includes other groups [eg employees / officials]. We process personal data for a number of purposes, such as administration and communication. It is critical that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in the Act.

DEFINITIONS

In order to appreciate fully the requirements of the Act, it is important for you to understand the meaning of certain key words and phrases which are used within the Act.

These include the

- ❖ **data** which is
 - information that is processed electronically [eg by computer],
 - recorded manually [eg on paper] with the intention of being processed electronically,
 - recorded as part of a relevant filing system [see below], or is
 - none of these, but forms part of an accessible record.
- ❖ **Data Controller:**

This is the organisation that determines the purposes for which and the manner in which, personal data is processed.

The Province, through the Provincial Grand Secretary / Scribe E, is the data controller; the Designated Users are not data controllers.
- ❖ **Data Processor:**

This is an external organisation that we appoint to process personal data on our behalf.

Examples of these might include an IT outsourced services provider, an external payroll bureau or Masonic Unit undertaking work outside the Provincial Office.
- ❖ **Data Subject:**

A living identifiable individual, about whom we process personal data.
- ❖ **Information Commissioner,**

who is the supervisory authority responsible for enforcing the provisions of the Act in England and Wales;
- ❖ **Personal data,**

which is the data relating to a living individual who can be identified from that data or from data and other information which is in our possession, or likely to come into our possession. Personal data includes opinions and indications of our intentions towards an individual.
- ❖ **Processing,**

has a wide meaning and covers virtually any action relating to personal data, such as obtaining, recording, holding, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying personal data.
- ❖ **Relevant Filing System,**

is a set of manual information [ie paper files] relating to individuals which is structured by reference to any individual or criteria relating to them in such a way that specific information relating to a particular individual is readily accessible.
- ❖ **Sensitive Personal Data,**

means information relating to his / her

 - racial or ethnic origin of the data subject,
 - political opinions,
 - religious beliefs or other beliefs of a similar nature,
 - trade union membership,
 - physical or mental health or condition,
 - sexual life,
 - commissioning or alleged commissioning by him /her of any offence, and
 - any proceedings for any offence committed or alleged to have been committed by him / her and the disposal of such proceedings or the sentence of any court in such proceedings.

THE PRINCIPLES

First Principle

Personal data must be processed fairly and lawfully and must not be processed unless

- ❖ at least one of the conditions in Schedule 2 is met and
- ❖ in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first and possibly most important of all the principles. It requires us to process personal data fairly and lawfully. Each of these requirements is considered in turn below.

Lawful processing

The Act prohibits the processing of any personal data unless that processing can be justified under one of a number of conditions which are set out in Schedules 2 and 3 of the Act. It is worth remembering the very broad definition of 'processing' which includes obtaining, disclosing, using and viewing.

You must justify your processing of all personal data under one of the conditions set out in Schedule 2. If you cannot find a condition that justifies your processing then that processing must not take place.

Schedule 2 conditions

- 1 The data subject has given consent to the processing.
- 2 The processing is necessary in order to enter into or perform a contract with the data subject.
- 3 The processing is necessary for compliance with any legal obligation to which The Province 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 for the
 - ❖ administration of justice,
 - ❖ exercise of any functions conferred on any person by or under any enactment and
 - ❖ exercise of any other functions of a public nature exercised in the public interest by any person.
- 6 The processing is necessary for the purposes of legitimate interests pursued by the data controller, or by the third party or parties, to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

When considering the above conditions remember the broad definition of processing. For example, obtaining consent to processing means obtaining consent to the disclosure, collection, use, destruction etc of personal data.

In addition, when you are processing sensitive personal data, you must, also, justify that processing under one of the conditions in Schedule 3.

This is a safeguard which recognises the sensitive and sometimes confidential nature of this category of personal data.

The most relevant Schedule 3 conditions are set out below.

Schedule 3 conditions

- 1 The data subject has given explicit consent to the processing.
- 2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Province in connection with employment.
- 3 The processing is necessary in order to
 - ❖ protect the vital interests of the data subject or another person, where, in a case, where cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - ❖ 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 is
 - ❖ necessary for the purposes of, or in connection with, any actual or prospective legal proceedings,
 - ❖ necessary for the purpose of obtaining legal advice, or
 - ❖ otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- 5 The processing is necessary for the [a] administration of justice, or [b] exercise of any functions conferred on any person by or under any enactment.
- 6 The processing
 - ❖ includes sensitive personal data consisting of information as to racial or ethnic origin,
 - ❖ 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
 - ❖ is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- 7 The processing
 - ❖ is in the substantial public interest,
 - ❖ is necessary for the purposes of the prevention or detection of any unlawful act, and
 - ❖ must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.
- 8 The processing
 - ❖ is of sensitive personal data consisting of information as to religious beliefs or other beliefs of a similar nature, or physical or mental health or condition,
 - ❖ is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons holding different religious beliefs, or different states of physical or mental health, or conditions, with a view to enabling such equality to be promoted or maintained and
 - ❖ does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject and

- ❖ does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

Remember: unless you can justify your processing of sensitive personal data under both Schedules 2 and 3, you must not process the data.

Fair Processing

The second requirement of the first principle is that personal data must be processed fairly. In broad terms, what this means is that we must ensure transparency of processing so that data subjects are aware of who is processing their personal data and why.

We achieve this by giving data subjects a data protection notice which meets the following requirements:

Content of data protection notice:

- ❖ The identity of the data controller [ie the Province]
- ❖ The purposes for the processing.
- ❖ Any other information that is necessary to make the processing fair [such as any recipients of the data and their purposes, a reminder of the data subject's right of access and correction and whether any of the information we are asking for is mandatory or voluntary]

Timing of data protection notice:

- ❖ The data protection notice must be given to the data subject at the right time. Where we obtain personal data directly from the data subject [eg as a result of a telephone call, or online journey] we must give the notice to the data subject at the time we obtain his data.
- ❖ Where we obtain personal data about a data subject from a third party source [eg a family member] we must provide the data protection notice as soon as reasonably practicable after we have started processing his data [unless it would be a disproportionate effort to do so].

Position and format of Data Protection Notice:

- ❖ The Data Protection Notice must be reasonably prominent and in reasonably legible font.
- ❖ The Data Protection Notice must be included at every point where we collect personal data, such as application forms and websites.
- ❖ If, for example, the data protection notice is provided online, it must be positioned so that it can be seen and not hidden behind a hypertext link.

You can obtain copies of our standard and current Data Protection Notices from the Provincial Grand Secretary. These notices have been drafted to take account of the kind of processing that we do. You should use the data protection notices whenever you obtain personal data. You must not modify any of these notices without prior authority. These notices have been drafted so that they comply with the Act and any modification on your part could change that. If you think the notices do not cover your particular processing activities you must discuss this in the first instance with the Provincial Grand Secretary.

Second Principle

Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

The second data protection principle sets out two requirements:

- ❖ personal data must be obtained only for one or more specified and lawful purposes. Our data protection notices will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose [unless the data subject gives his consent].
- ❖ personal data must not be further processed in any manner incompatible with the purpose or purposes for which the data were obtained. A breach of this principle could also result in a breach of the first principle.

Third Principle

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

The third data protection principle requires that personal data must be adequate, relevant and not excessive. You must, therefore, ensure:

- ❖ you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose
- ❖ you do not hold personal data on a 'just-in-case' basis because you think it might be useful in the future but without having any clear idea of the future purpose.
- ❖ you keep data up to date [or else originally adequate data might cease to be adequate / relevant.]
- ❖ you do not keep data for too long [otherwise those data may cease to be relevant and become excessive].

Fourth Principle

Personal data must be accurate and, where necessary, kept up to date.

Personal data will be inaccurate if they are incorrect or misleading as to any matter of fact [eg an incorrect name or address]. If you are inputting data onto our system and are unsure as to the accuracy of certain information [eg because you cannot read the handwriting or because it looks like an obvious mistake or omission], you should try to get in touch with the data subject to clarify the issue.

We will not be in breach of this principle, even if we are holding inaccurate data if:

- ❖ we accurately recorded those data when we received them from the data subject or a third party and
- ❖ we took reasonable steps to ensure the accuracy of those data and
- ❖ if the data subject has notified us that the data are inaccurate, we have taken steps to indicate this fact [eg by making a note that we have received an objection].

You must take reasonable steps to keep data up to date to the extent necessary. The purpose for which data are held will determine whether they need to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

Fifth Principle

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

You should review the personal data which you hold on a regular basis and delete any data which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. You should also consider the type of relationship which The Provincial Grand Lodge of East Lancashire has with the data subject and whether there is an expectation that we will retain data for any given period of time [eg our employees would expect us to retain their data for a period of time after they had left].

Sixth Principle

Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

The rights which are referred to in the sixth principle are the data subject's rights in relation to:

- ❖ access to his personal data,
- ❖ preventing processing likely to cause damage or distress,
- ❖ preventing processing for the purposes of direct marketing,
- ❖ automatic decision-taking.

If you receive a request in writing from an individual mentioning any of the above rights, you must pass that request promptly to the Provincial Grand Secretary / Scribe E, as there are strict timescales within which we must respond.

Seventh Principle

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

The seventh principle requires the Province to take technical and organisational measures to protect personal data which we process:

- ❖ technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; and encryption all of which we have in place and manage through our IT department;
- ❖ organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff on the care and handling of personal data all of which you are responsible for complying with and applying to your daily routine.

The Act imposes upon the Province, additional obligations if we use third parties to process personal data on our behalf. Some of these third parties may have access to, or need to process, personal data on our behalf. If so, they will be acting as our data processors and the Act requires us to

- ❖ put in place a contract in writing with each of our data processors under which they agree to act only on instructions from us,
- ❖ include the right to audit our data processors to ascertain compliance with the data protection requirements of the processing contract and
- ❖ ensure that the data processor agrees to comply with obligations equivalent to those imposed on us by the seventh principle.

If you are responsible for the selection, appointment or use of data processors, you must ensure that you only select those processors that are able to provide us with sufficient guarantees in respect of the technical and organisational measures they will apply to the processing of our personal data. Furthermore, if you are responsible for the drafting or negotiation of contracts with data processors, you must ensure those contracts contain all applicable data protection provisions.

Do not hesitate to seek further advice from the Provincial Grand Secretary /Scribe E.

Eighth Principle

Personal data must 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.

You must not transfer any personal data to any country outside the European Economic Area [EEA], unless you are authorised to do so.

The EEA comprises the EU Member States plus Iceland, Norway and Liechtenstein.

If you need to transfer personal data to a country outside the EEA, you must consult with the Provincial Grand Secretary / Scribe E, who will advise you further on how to comply with the adequacy requirements of the eighth principle.

DATA SUBJECT RIGHTS

The sixth data protection principle requires us to comply with the rights of data subjects. It is important for you to familiarise yourself with these rights so that you may be able to identify them more easily. Each one is described below.

Right of subject access

Data subjects have a right of access to their personal data. A request for access will usually include a request for specific or general information relating to the applicant. If we receive such a request we must provide a description of the

- ❖ personal data relating to that data subject,
- ❖ purposes for which the data are being processed,
- ❖ recipients of the data,
- ❖ information constituting the personal data and
- ❖ source of those data [if available].

The Act lays down timescales within which we must comply with a request and requirements regarding how the information must be supplied.

You should forward the request to the Provincial Grand Secretary.

Right to prevent processing likely to cause damage or distress

Data subjects have the right to ask us not to process their personal data if

- ❖ the processing of those data in a particular way or for a particular purpose is causing, or is likely to cause, substantial damage or substantial distress to that data subject or another person; and
- ❖ that damage or distress is, or would be, unwarranted.

You can usually identify a request to exercise this right because it will ask us to stop processing personal information about the individual. The Act lays down timescales within which we must comply with such a request.

If you receive a request to stop processing you must forward it promptly to the Provincial Grand Secretary. You should not attempt to deal with a request on your own.

Additional data subject rights

In addition to the rights specifically referred to in the sixth principle, data subjects also have the following rights which include the right to

- ❖ ask the Information Commissioner to carry out an assessment as to whether or not the Province is processing in accordance with the Act.
This means the data subject has the right to make a complaint to the Commissioner and ask him to investigate.
The Commissioner is obliged to consider all such requests and this could result in an investigation of our processing activities,
- ❖ take legal action against the Province in the courts and claim compensation for any damage [or damage and distress] the data subject has suffered as a result of a breach of the Act and
- ❖ to apply to court for an order to rectify, block, erase or destroy inaccurate personal data and any expression of opinion based on those inaccurate data.

Consequences of non-compliance

If we are found to be in breach of the Act, the Information Commissioner may issue enforcement proceedings against us which could result in our being prevented from further using personal data, or be required to change our processing procedures, or have other conditions imposed upon us in respect of the processing of personal data.

Enforcement action will usually have a cost and time implication for the business.

However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases commercially.

Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals.

Affected data subjects may also take legal action against us and claim compensation for any breaches of the Act on our part that have resulted in damage [or damage and distress] to the data subject.

In certain circumstances, a negligent or deliberate breach of the Act could result in criminal liability not just for the Province but for our employees, also.

For these reasons it is essential to comply with the provisions of the Data Protection Policy and this Guidance.

Contacts and responsibilities

If you have any queries regarding the Data Protection Policy, this Guidance or compliance with the Act in general, please contact the Provincial Grand Secretary for further advice.

The Data Protection Policy and this Guidance will be updated from time to time by the Provincial Grand Secretary to reflect any changes in legislation or in our methods or practices.

*Issued by the Provincial Grand Secretary
August 2008*

DATA SECURITY POLICY

INTRODUCTION

- 1.1 The Data Protection Act 1998 [the Act] imposes certain obligations upon the Province in relation to the processing of personal data. These obligations are contained within eight data protection principles. The seventh principle relates to data security and requires us to take appropriate technical and organisational measures to safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
For more information on the other principles please refer to the Data Protection Policy.
- 1.2 We recognise the importance of personal data to our business and the importance of privacy rights to individuals about whom we process personal data. This Policy is intended to assist our staff to comply with the requirements of the seventh principle. This Policy is not limited to protecting personal data but extends to all information which we hold. References to 'personal data' should be read to include information of any kind that is used within the business, including confidential information.
- 1.3 The Act includes a number of defined terms which are used in this Policy. These terms include:
- ❖ **Data Subjects,**
means individuals about whom we process personal data.
 - ❖ **Personal Data,**
means data which relates to a living individual who can be identified from the data or from data and other information which is in our possession, or likely to come into our possession.
 - ❖ **Processing,**
means virtually anything we do with personal data such as collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction.
 - ❖ **Sensitive Personal Data,**
means personal data about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, commission or alleged commission of an offence, or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings.

References to 'we' and 'us' refer to the Province.

YOUR RESPONSIBILITIES

- 2.1 You must familiarise yourself with this Policy and implement its requirements within your Districts and working practices. Please refer to the Data Protection Policy for guidance on the requirements of the Act in general. You can obtain a copy of the Data Protection Policy from The Provincial Grand Secretary Scribe E.
- 2.2 You have an obligation to comply with this Policy.

Any failure to comply with this policy may be a disciplinary offence which could result in dismissal or removal from office. Negligent or deliberate breaches could result in criminal liability for you personally or action being taken under the masonic code of conduct.

POLICY

- 3.1 The seventh data protection principle requires the Province to take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- 3.2 In order to comply with the seventh principle you,
- ❖ must comply with the technical and organisational measures set out in the Annex to this Policy whenever you process personal data,
 - ❖ must consider the nature of the personal data you are processing and determine whether the technical and/or organisational measures are commensurate to the harm that might result if there were a security breach. If the data are also confidential or sensitive personal data, an additional level of security will be required:
 - Examples of confidential information may include personnel data and financial information.
 - Examples of sensitive personal data may include information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, commission or alleged commission of an offence, or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings].
 - ❖ should only hold personal data for as long as it is required for the purpose for which those data were originally collected. Once the data is no longer required, you must destroy or delete the data securely;
 - ❖ must immediately report all actual or suspected security breaches to the Provincial Grand Secretary / Scribe E. Where the breach involves personal data, you should also notify the Provincial Grand Secretary / Scribe E.
- 3.3. The Province is responsible for taking reasonable steps to ensure the reliability of employees and officers who have access to personal data. If you are responsible for the recruitment of staff [whether permanent, temporary or contract], you must assist in the compliance by
- ❖ screening/vetting all new staff,
 - ❖ ensuring all new staff sign terms and conditions which include confidentiality and security obligations,
 - ❖ taking up references for all new staff and
 - ❖ ensuring new staff are trained on the care and handling of personal data when they join [eg as part of their induction training].
- 3.4. As part of the Province's obligation to ensure the reliability of employees who have access to personal data, we must provide training on the requirements of the Act. If you are responsible for training staff [whether permanent, temporary or contract], you must ensure that periodic training sessions [including refresher courses] are provided to staff on data protection topics, including the care and handling of personal data and security requirements.
- 3.5. The Province is required to take additional security measures whenever it uses third parties to process personal data on its behalf. Third parties may include IT contractors, providers of hosting services for our websites, outsourced service providers, payroll providers, computer maintenance providers, disaster recovery service providers. These third parties are referred to as 'data processors'.

If you are responsible for the selection or appointment of any data processors, or are involved in contract negotiations with data processors you must

- ❖ make sure you only select data processors that provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the processing of personal data,
- ❖ enter into a contract in writing with each data processor.
It is important to do this before the processing actually begins.
- ❖ ensure that each processing contract makes it clear that data processors must only act on instructions from the Province
We are responsible for the processing of all personal data, even if it is carried out on our behalf by a data processor. We must, therefore, maintain control over such processing at all times;
- ❖ ensure that each data processor agrees to take appropriate technical and organisational measures to protect any personal data that it processes on our behalf from unauthorised or unlawful processing, accidental loss, destruction or damage. It is important that we specify any measures that must be taken;
- ❖ ensure that we have the right to check the data processor's compliance with the terms of any processing contract. This may involve auditing the data processor from time to time to make sure that it is processing in accordance with our instructions and the security measures we have specified, as well as any other data protection related requirement of the Act,
- ❖ check to see if the data processor will be holding personal data on our behalf and whether or not we do not, also, have a copy of those data. We must make sure the processing contract includes a provision that requires the processor to assist us promptly with any *subject access request [a request received from a data subject asking for access to personal data which we process about him / her] which we might receive in relation to any of the data held by the data processor,
- ❖ must ensure that upon termination of the processing contract, the processor promptly returns or destroys the personal data as directed by us,
- ❖ if the data processor will be collecting personal data on our behalf, the processing contract must include an obligation upon the processor to give our standard data protection notice [which the processor is not allowed to modify] to all individuals about whom the processor collects personal data.

3.6 If the data processor proposes to use sub-processors to assist with the processing services, you should seek advice from the Provincial Grand Secretary / Scribe E., as this will have consequences for the Province and specific provisions will need to be included in the processor agreement.

3.7. Whilst we delegate some our processing activities to a data processor, it is important to remember that just because we are taking a wider view point, does not mean that we can delegate our responsibility to comply with the Act.

CONTACTS AND RESPONSIBILITIES

4.1. If you have any queries about this Policy, please contact the Provincial Grand Secretary / Scribe E.

4.2. We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information Commissioner.

*Issued by the Provincial Grand Secretary
July 2008*

ANNEX

TECHNICAL AND ORGANISATION MEASURES

Technical Security Measures

1. Protection against malicious software/viruses [eg software should not be installed from removable media or downloaded from the internet without virus checking it first]
2. Backing up data [eg regular back ups should be taken of all data on our systems; data should not be stored on local drives or removable media as these will not be backed up]
3. Encryption
4. Secure exchange of information
5. User access controls [eg passwords should be allocated to all users; passwords should be changed on a regular basis; passwords should not be pinned up next to the computer or anywhere else where they could be seen; computers should have password activated screen savers that can be turned on whenever the user is away from his or her desk; passwords should include a mixture of letters and numbers; avoid passwords that are easy to guess such as your name or date of birth; different access should be allocated to different users depending on job description and need to access personal or confidential data; different access rights should be allocated to individuals who have a need to modify personal or confidential data; read and write privileges should be allocated depending on job description and need]
6. Network access controls [including passwords]
7. Monitoring system access and use
8. Guidance on mobile computing [eg do not leave laptops unattended in cars or in public places or on top of desks left unattended overnight]
9. Disaster recovery [eg ensure copies of personal data are stored off site in a secure and fire-proof location; business continuity plan should be created; disaster recovery and business continuity plans should be tested periodically]
10. Secure destruction or deletion of data and secure disposal of computer equipment and removable media [eg where you are destroying personal data or confidential information make sure that you do so securely by using a high spec shredder or confidential waste disposal agent; make sure that all hard drives are erased on all computers before their disposal]
11. Lockout mechanisms [eg system should automatically lockout when a user attempts to login using an incorrect password]
12. Security audits [eg check networks comply with security policies; identify any risk areas]
13. User authentication

Organisational Security Measures

14. Entry controls to premises [eg visitors must sign in at reception]
15. Secure access to computer facilities [eg keypads or locks on doors; authorised personnel allowed access only]
16. Positioning equipment so as to prevent screens from being overlooked [eg make sure that any personal data displayed on computer screens cannot be overlooked by passers-by]
17. Securing equipment when off-site
18. Secure disposal of equipment or its re-use/re-conditioning
19. Procedure should be put in place to handle any breaches of security [eg policy should identify who is responsible for handling these breaches; audit trails should be available to show any unauthorised access; staff should be trained to report actual or suspected breaches immediately]
20. Training [eg on the care and handling of personal data; on security systems; on the procedure for handling security breaches; training records should be maintained for all staff; training should be refreshed periodically; employees should be contractually bound to attend all relevant training sessions; training can be delivered via the intranet or internet]

H Alan J Garnett
Provincial Grand Secretary
July 2008

f:\data protection act\east lincs\policy document, august 2008.doc