Data Protection Policy
07/10/2008

CONTENTS

PART A

GENERAL CONDITIONS

1	INTRODUCTION	**3**
2	WHAT IS PERSONAL DATA?	**3**
3	WHAT IS PROCESSING?	**4**
4	THE RULES FOR PROCESSING PERSONAL DATA	**4**
5	COMPLIANCE MEASURES	**9**
6	EXEMPTIONS	**10**
7	DATA PROTECTION FOR EMPLOYEES	**11**
8	MONITORING	**12**

PART B

EMPLOYMENT RULES

1	THE RULES FOR PROCESSING PERSONAL DATA	**13**
2	CONSENT	**15**
3	MONITORING	**17**
4	CONCLUSION	**17**

PART A

DATA PROTECTION POLICY

1. INTRODUCTION

The Data Protection Act 1998 ("DPA") gives rights to individuals, including employees, about whom information or "personal data" is obtained or processed, whether manually or electronically. This policy does not distinguish between manual and electronic data.

This policy describes the requirements for the processing of personal data by S4C to meet our legal obligations.

S4C is committed to fulfilling its obligations under data protection legislation in respect of all processing of personal data in connection with its business and in so doing meeting the expectations of our employees, viewers, suppliers and the regulatory authorities.

In order to ensure a consistent approach is adopted throughout S4C to compliance with the DPA an individual has been appointed to the role of the S4C data protection officer ("the Data Protection Officer"). Details as to the current Data Protection Officer can be obtained on the S4C intranet site or by contacting the HR department.

2. WHAT IS PERSONAL DATA?

Personal data is information which relates to a living individual (this includes partnershipbut not corporate entities such as companies) who can be identified from that information, whether or not in conjunction with any other information. Common examples of personal data which may be used by S4C in its day to day business include names, addresses, telephone numbers and other contact details, CVs, performance reviews, salaries, royalty payment details and statements of opinion or intention regarding individuals. Some information is considered to be sensitive personal data ("Sensitive Personal Data").
This includes information relating to:

- race or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or conditions;
- sexual orientation/behaviour; or
- information relating to the commission or alleged commission of any offence and any related court proceedings, including the disposal of or sentence in those proceedings.

Where information amounts to Sensitive Personal Data more rigorous rules apply in terms of justification of any processing of such information.

If in doubt as to whether any processing intended to be undertaken is within the remit of the notification then advice should be sought from the Data Protection Officer prior to commencement of such processing (see Section 4.3 for details as to the permitted processing as set out in the notification made by S4C).

3. WHAT IS PROCESSING?

S4C will be processing personal data if it holds personal data and/or carries out any operation relating to that information such as altering or deleting it, accessing, downloading, reviewing or transferring it.

It is irrelevant whether the information is stored as a manual record or is automatically processed (i.e. computer or word processed).

Where personal information is held in manual form only, it will not be covered by the DPA if it is not contained within a structured filing system (in that information is held in a manner whereby it can be located by way of a search against the individuals name) Therefore, for instance, information held on a file in date order only will not be within a structured filing system and therefore if only held in that form will not be subject to the DPA rules set out below. Before concluding that information is not held in a relevant filing system advice should be sought from the Data Protection Officer

4. THE RULES FOR PROCESSING PERSONAL DATA

Disclosure and use of personal data held by S4C is governed by the following rules in order to ensure compliance with the DPA.

4.1 Notification

S4C is required to notify the Information Commissioner (formerly known as the DataProtection Commissioner) about the processing of personal data carried out by S4C. S4C has notified its processing accordingly and has appointed a Data Protection Officer to review and co-ordinate the processing of personal data within S4C in accordance with the DPA and recommended good practice. S4C can only lawfully process data within the remit of its notification (please see section 4.3. below for further information on this point). Further details of the Data Protection Officer's role are set out later in this policy.

4.2 Use of Personal Data must be Fair and Lawful

S4C must ensure that:

- wherever possible individuals are advised of the personal data which has been obtained or retained, its source and the purposes for which the personal data may be used or disclosed; and

- ensure, in most cases, that there is consent to use the information

If details about the intended processing are known to the individual at the time the personal information is collected, then, in the main, there will be deemed to have been a general consent given by the individual when furnishing the information. If the information is not received directly from the individual to whom the data relates (i.e. from a third party) then it is important to ensure that

the individual is given all the relevant information above and S4C has authority to use such information. However, S4C will generally need the explicit consent of the individual to process Sensitive Personal Data and in this circumstance consent cannot be deemed to have been given. If there is no explicit consent or the information has not been received directly from the individual, S4C will not process this information unless it obtains the relevant consents or is otherwise lawfully entitled to do so. Details as to justification for processing such data without consent are set out in sections 2.1 and 2.2 of Part B of this Policy (as set out below)

If the reasons for processing that data change, then the data subject must be notified at that point.

Occasionally, specific business needs and/or another specific provision of the DPA, can justify processing without consent. However, only the Data Protection Officer may authorise any such processing without consent.

When dealing with Sensitive Personal Data consideration should at all times be given to the security of such information. In particular where such information is issued (subject to the DPA rules) by S4C to the data subject or an authorised third party then it should be done in such a manner so as to maintain the security of such information.

Sensitive Personal Data should not be sent by fax unless it is to a confidential or direct fax number, the fax is marked confidential and the recipient has been notified in advance of it being sent. If Sensitive Personal Data has to be sent by email, advice should always be sought from the Data Protection Officer

4.3 **Personal Data must Only be Used for Specified Lawful Purposes**

S4C must only use personal data:

- for a lawful purpose; and
- where it is covered by S4C's notification to the Information Commissioner (see below).

The main purposes for which S4C is covered under its notification are:

- Staff administration;
- Advertising, marketing and public relations;
- Accounts and records;
- Information and databank administration;
- Crime prevention and prosecution of Offenders
- Fundraising;
- Realising the objectives of charitable organisation or voluntary body;

- Journalism and media; and
- Research

S4C's notification number is Z7331203. This notification lists all the purposes for which S4C may process personal data. Any additional processing must be notified to the Information Commissioner with the notification being updated to reflect such additional processing A copy of the notification may be obtained from the Data Protection Officer or from the Register of Data Controllers held on the Information Commissioner's website (www.ico.gov.uk). If you have any doubt whether the purpose of any processing you may undertake is covered by the notification you must check with the Data Protection Officer.

Processing for any additional purposes must be approved in writing by the Data Protection Officer before that processing takes place.

Any employee or officer of S4C who has or intends to create their own system or record, for example a spreadsheet or database/card index, whether computerised or on paper which contains personal data, should ensure that such processing is consistent with the purposes set out within the S4C notification and compliant with the requirements of the DPA rules. If there is any doubt as to whether such a record/system complies with the requirements of the DPA rules then advice should be sought from the Data Protection Officer.

Provided that the identification of individuals cannot be ascertained or is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data, i.e. surveys, manpower figures.

4.4 **The Use of Personal Data must be Justified**

The personal data processed by S4C must be adequate, relevant and not excessive for S4C's legitimate operational purposes. Methods of data capture must:

- be specific to the particular processing purpose;
- obtain all personal information necessary on which to base any decision that is to be taken for the processing purpose;
- not collect personal data that is simply "nice to have", which is otherwise not necessary for the processing purpose for which the individual has provided his/her details, or which is to be used for another purpose (i.e. marketing) about which the individual has not been informed. If information about other family members, interests and hobbies are not strictly relevant to any purpose about which the individual has been informed, then this information should not be collected; and
- ensure that the data subject is informed at the time the information was collected of the processing purpose or (where applicable) that consent is subsequently obtained.

4.5 **Personal Data must be Accurate**

The best way to ensure that the information is accurate is to check this with the individual at the time it is collected. Some personal information collected may change from time to time, such as address and contact details, bank accounts and employment. If S4C takes a decision based on inaccurate information or forwards information to the wrong address it is conceivable that this may cause some harm to the individual. It is therefore important that, where necessary, information is kept up to date.

If personal information is held or used for long periods of time there is the possibility that some or all of the information held may become inaccurate. Regular reviews of the information must be carried out to ensure its accuracy e.g. to ensure that marketing databases and mailing lists do not contain details of individuals who have registered with a preference service (e.g. mail or telephone) and that notifications of changes to data received from a data subject have been actioned.

4.6 **Data retention - Personal Data must only be retained for as long as it is necessary for the purpose(s) for which it is being processed by S4C**

Information which amounts to personal data must only be held by S4C for specific purposes and consideration must be given as to the need to maintain such information once that purpose no longer applies. For example, if information is held documenting a relationship with an individual it will be necessary to consider when that relationship ceases to exist whether the data held, regarding that individual, can still legitimately be held by S4C. It should be noted that there may be a number of reasons for retention of data even where the relationship no longer exists (e.g. information could be retained for the relevant statutory time - limits relating to possible legal actions or in the context of an employee for the purpose of pension arrangements). If in doubt seek guidance from the Data Protection Officer.

4.7 **Personal Data must be Processed in Accordance with Individuals' Rights**

Individuals have rights in relation to information processed about them and S4C is required to process data about such individuals in accordance with their rights. These include the right to:

- have information made available on request (please see Section 4.11 below);and

- request that S4C does not process information which will or is likely to cause substantial and unwarranted damage or distress to the individual.

4.8 **Appropriate Security must be Applied to all Personal Data**

S4C must have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal information. Special security measures may be required to be put in place in the case of Sensitive Personal Data.

Where personal information is required to be passed to third parties who process that information on behalf of S4C, such processing may only be undertaken where they have signed S4C 's Data Processing Contract. Advice should be obtained from the Data Protection Officer as to the appropriate contractual documents to use.

Generally information released to a third party for processing on its own behalf, must only be released with the individual's consent. In the absence of consent advice should always be sought from the Data Protection Officer before personal data is disclosed to any third party.

Personal data must only be disclosed to those authorised to see it.

Under no circumstances must information be released about an individual to any personrequesting this information by phone, fax or post, unless the identity of the person making the request, and that they are entitled to receive the information requested, has been confirmed. Please note that parents (unless in relation to children under 16), spouses, partners and children are not entitled to information about other family members or partners etc.

If in doubt the information should not be released and the request should be referred to the Data Protection Officer

4.9 **Transfers outside the European Economic Area**

The DPA prohibits the transfer of personal data outside of the EEA except in limited circumstances. As a result S4C will only transfer personal information outside the European Economic Area where either consent from the individual in question to such a transfer is obtained, where the transfer is to a country (other than one which has been deemed adequate by the European Commission), where necessary steps have been taken to ensure that the information transferred is kept secure or where a specific exemption to this rule applies (please see section 6 below regarding the research and media exemptions).

The European Economic Area currently includes Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden and UK. The countries currently deemed adequate include the USA (but only where the recipient is a company that has signed up to the Safe Harbor principles), Argentina, Switzerland and Canada.

In order to ensure compliance with the DPA rules regarding data transfer, all transfers of personal information outside the European Economic Area (other than those covered by the exemptions set out in section 6 below) must be approved first by the Data Protection Officer.

4.10 **Direct marketing**

In addition to the rules set out in the DPA regarding use of personal data, specific rules apply in respect of use of data for marketing purposes by electronic means (e-mail, fax, telephone and SMS). These rules are set out in the Privacy and Electronic Communications (EC Directive) Regulations 2003. Advice should be

sought from the Data Protection Officer if you are unclear as to the rules relating to the intended use of any personal data for direct marketing purposes.

S4C must not direct market any individuals (including business partnerships) unless it has obtained the prior consent of those individuals. This consent can be obtained at the time the information is provided by the individual. S4C will comply with any request by an individual not to receive direct marketing information.

Additionally, the Telephone Preference Service and Fax Preference Service must be checked prior to contacting (for marketing purposes) any individual by telephone, email, SMS or fax. Elections not to receive marketing by fax, email, SMS or telephone must be complied with.

4.11 **Access to Information**

S4C has a central procedure for dealing with all requests for access to personal information, in accordance with the provisions of the DPA. Generally, if such a request is made, S4C must:

4.11.1 advise the data subject whether it (or someone on its behalf) is processing any personal data concerning them;

4.11.2 if so, give the data subject a description of that personal data, the purposes for which is being processed and the recipient or classes of recipient to whom it is or may be disclosed;

4.11.3 inform the data subject, in an intelligible and permanent format (unless the cost of such permanent format would be disproportionate), of the information contained in that personal data and its source; and

4.11.4 advise the data subject of the logic involved where a decision relating to or significantly affecting the data subject is made on the basis of processing that personal data by automatic means.

All requests will be dealt with by the Data Protection Officer within 40 days of receipt of the request from the individual in writing, together with a £10.00 access fee made payable to S4C. In order to ensure consistency in terms of responses made, any requests received must be passed immediately to the Data Protection Officer, whether from employees or external sources.

In addition to the rights of access set out in the DPA, S4C Staff members may also view, in conjunction with a member of the HR department, their personnel files as held by S4C's HR department and take a reasonable number of copies of the same.

5. COMPLIANCE MEASURES

In order for S4C to comply with this policy, all employees and officers of the Company must only process personal data in a manner which is compliant with this Data Protection Policy.

6. EXEMPTIONS

The notified measures set out in Section 4.3. above include "Research" and "journalism" and processing for these purposes is subject to a number of exemption to the general rules that apply under the DPA.

6.1 Research

Where information that amounts to personal data is processed by S4C for research purposes only (which under the DPA covers research for historical or statistical purposes) the following exemptions to the DPA rules apply:

- further processing of personal data for research purposes only is not in itself to be regarded as incompatible with the original purposes for which such data were obtained;
- it can be held indefinitely (notwithstanding the requirements in relation to retention of personal data as referred to in section 4.6 above)
- the access rights of data subjects as referred to in section 4.11 do not apply to personal data processed for such research purposes The exemptions to the usual DPA rules as detailed above will not apply if the data in question is processed in a manner other than purely for research purposes. In addition in order to be covered by the exemption the data must not be processed (in terms of the research undertaken) in a manner which causes or is likely to clause significant distress or damage to the data subject. This exemption should only be applied if sign off has been received from the Data Protection Officer.

6.2 Journalism, Literature or Art

Personal data which is processed by S4C for journalistic, literary or artistic purposes are generally exempt from the majority of the DPA rules, although the obligation on S4C in relation to putting in place adequate security of personal data it processes (the Seventh Data Protection Principle) still applies, even where the purpose of the processing is for journalistic reasons.

The exemption in terms of processing for journalistic reasons will only apply if it can be shown that : -

- the processing is undertaken with a view to the publication by S4C or a third party of journalistic, literary or artistic material;
- it can be shown that S4C had reasonable belief that publication is in the public interests (taking into account the importance of freedom of expression to the public interest); and
- S4C can demonstrate that it is/was reasonable to conclude that compliance with the exempted provisions of the DPA as detailed above would be incompatible with the intended processing for journalistic, literary or artistic purposes.

As a result, sign off from the Data Protection Officer must be obtained before reliance is placed on this exemption.

7. DATA PROTECTION FOR EMPLOYEES

Initial personal data relating to employees is ordinarily obtained from job application forms submitted to S4C and thereafter principally from employees themselves by way of annual appraisal.

Requests for data concerning employees by external sources which have been authorised by S4C are:

7.1 Requests from agents authorised by the employee who is the subject of the data e.g. mortgage requests, references. However, confirmation should be sought from the employee that the information is to be released and if possible, the employee's written consent should be obtained.

7.2 Requests made for the purposes of law enforcement (i.e. for the prevention or detection of crime, the assessment or collection of any tax or duty or the assessment or collection of any liability via the Child Support Agency). Disclosure is only allowed where failure to make disclosure would be likely to prejudice one of those purposes. In all cases written evidence should be obtained from the Police, HM Revenue and Customs and the Child Support Agency as to the purpose of the request.

7.3 Requests for any other compulsory legal processes.

7.4 Requests, if urgently required, for the prevention of injury and damage to health.

7.5 Requests required by authorised officials or representatives of recognised trade unions. However, confirmation should be sought from the employee that the information is to be released and if possible, the employee's written consent should be obtained.

7.6 Requests required by specifically identified external sources e.g. pension administrators, in order to administer S4C's internal benefit schemes.

NB. All staff should endeavour to restrict disclosures requested from outside S4C to those required by law as much as possible.

Employees are, at reasonable intervals (which S4C deems to be every six months) entitled to have access to personal data held about them which is not excluded data (see below). They are also entitled to be informed of the purpose for which the data is being or is intended to be used and the likely recipients (or class of recipients). The following information is excluded from this right to access:

- Confidential references given by S4C. References received by the Company arenot automatically excluded under this exemption but may be similarly protected as disclosing information relating to identifiable third parties as set out below.

- Personal data processed for the purposes of management forecasting or management planning to the extent that disclosure would be likely to prejudice the conduct of that business or activity only.

- Personal data which consists of records of the intentions of the Company relating

to any negotiations with the employee to the extent that disclosure would be likely to prejudice those negotiations only.

- If, in order to comply with a disclosure request, S4C would need to disclose information relating to an identifiable third party then disclosure is not required unless the third party has consented or it is otherwise reasonable to comply with the request without such third party consent. Failing these options, the data must be edited prior to disclosure so that the identity of third parties is not discernible. If the information sought is a health record and the third party concerned is a health professional who has compiled or contributed to that health record then disclosure should be made.

The employee will not be able to prevent processing however, if the processing is necessary for the performance of a contract to which the employee is a party.

8. MONITORING

S4C may undertake monitoring of incoming and outgoing communication in order to ensure that such communications are being used for legitimate business purposes of S4C.
Monitoring may be undertaken: -

- to establish the existence of facts, to ascertain compliance with regulatory or selfregulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),
- to prevent or detect crime,
- to investigate or detect unauthorised use of telecommunications systems or,
- to secure, or as an inherent part of, effective system operation;
- monitoring received communications to determine whether they are business or personal communications;
- monitoring compliance with the S4C Email and Internet Usage Policy.

All such monitoring will be undertaken in compliance with the DPA rules, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

PART B

DATA PROTECTION RULES AND GUIDANCE FOR EMPLOYEES

1. THE RULES FOR PROCESSING PERSONAL DATA

All employees must carry out their duties in such a way so as to ensure that S4C complies with its obligations under the DPA as follows:

1.1 The Data Protection Principles

The eight Data Protection Principles must be observed. This means personal data must:

1.1.1 be processed fairly;

1.1.2 be processed for limited purposes as registered with the Information Commissioner;

1.1.3 be adequate, relevant and not excessive for those purposes;

1.1.4 be accurate;

1.1.5 not be kept longer than is necessary;

1.1.6 be processed in accordance with the Act;

1.1.7 be kept secure; and

1.1.8 not be transferred outside the EEA without necessary safeguards.

1.2 Consent to Processing

Personal data should only be processed where either consent has been obtained from the individual concerned or where, under the DPA rules, consent is not required. The rules for both obtaining consent and where consent is not required are set out in section 6 below.

1.3 Notice of Processing

Notice setting out details of the processing must be given to a data subject before any personal data relating to that data subject is processed. Any processing must be in accordance with that notice.

1.4 Processing Must be Covered by the S4C's Registration

You must only process data for the purposes which S4C has notified to the Information Commissioner (these purposes are set out in section 4.3 of Part A of this Policy).

1.5 **Only Record Necessary Data**

You should ensure that the methods by which you collect personal information are tailored to capture only personal information that is necessary for the purpose for which it has been provided by the individual. For example, if information about other family members, interests and hobbies are not strictly relevant to any purpose about which the individual has been informed, then this information should not be collected. This is particularly important where dealing with sensitive personal data. If in any doubt you should discuss and review methods of data capture with the Data Protection Officer. You should not collect personal data that is simply "nice to have", or which is to be used for another purpose (i.e. marketing) about which the individual has not been informed.

1.6 **Release of Data**

Under no circumstances should you release information about an individual to any person requesting this information by phone, fax or post, unless you have confirmed the identity of the person making the request and that they are entitled to receive the information requested. Please note that parents (unless in relation to children under 16), spouses, partners and children are not entitled to information about another individual. You should only release personal information to the individual to whom it relates. You may commit a criminal offence if you disclose the information to anyone who is not the individual without consent. If in doubt check with the Data Protection Officer. No matter what the reason – helping a friend, an address or contact number to a husband, an account enquiry by a partner – do not disclose the information unless you have the consent of the individual to do so.

1.7 **Requests by Individuals to See the Data Relating to Themselves**

If you receive a request by an individual (irrespective of whether this is received in writing or orally) to have copies of any information about the individual held by S4C (even where no reference is made to the Data Protection Act), the request must be referred immediately to the Data Protection Officer. Do not attempt to deal with the request yourself, or delay in sending it to the Data Protection Officer.

S4C Staff members may also view, in conjunction with a member of the HR department, their personnel files as held by S4C's HR department and take a reasonable number of copies of the same. This right is in addition to any staff members rights under the DPA to access to details of his/her personal data as held by S4C.

1.8 **Processing by Third Parties**

You must not pass any personal data to any third party (i.e. a party not under an employment contract with S4C) for processing unless you have confirmed that the necessary consent or contract is in place. If in doubt seek advise from the Data Protection Officer before releasing information for processing

1.9 **Sending Data Abroad**

Except in limited circumstances (such as for journalistic purposes - see section 6 of Part A of this Policy), you must not transfer data abroad without authorisation from the Data Protection Officer.

1.10 **Retention, Review and Destruction of Data**

As S4C is required not to keep information for any longer than is necessary for the purpose for which it is being processed, you must at all times comply with any instructions of the Data Protection Officer concerning the retention of data. If you know that information is incorrect or misleading as to any matter of fact or is out of date then arrange for it to be corrected as soon as possible. If a large volume of personal information/individuals are likely to be affected, you should liaise with the Data Protection Officer to ensure that the most cost effective method is adopted to update this information.

1.11 **Sending Sensitive Personal Data**

If you need to send Sensitive Personal Data by email, you must liaise with the Data Protection Officer, and where appropriate the IT department, to ensure appropriate security can be afforded to the information. Sensitive Personal Data may not be sent by fax unless it is to a confidential or direct fax number, the fax is marked confidential and the recipient has been notified in advance of it being sent.

1.12 **Creating Your Own Record System**

If you have created your own system or record, for example a spreadsheet or database/card index, whether computerised or on paper, which contains personal data you must ensure that the Data Protection Officer is aware of this processing and that appropriate security has been applied to this system or record.

1.13 **Working Away from the Premises**

If you work away from S4C premises due consideration must be given to compliance with the DPA rules and in particular the need for appropriate security measures to be put in place in respect of information. You should seek advice from the S4C HR department as to appropriate procedures for home working.

1.14 **Requests for Copies of Our Policies**

Any request received from any individual, employee, viewers or supplier for details of S4C Data Protection Policy or our security procedures must be referred immediately to the Data Protection Officer.

2. **CONSENT**

2.1 **When is Consent not Required?**

Provided that the individual concerned has been notified in writing that his/her data may be processed by S4C for the relevant purpose(s), then you may process

personal data (but not Sensitive Personal Data) without consent from the individual concerned as follows:

2.1.1 Where the processing is necessary for the performance of a contract with the person to whom the data relates. This includes administration of pay and benefits for employees and fulfilling customer orders.

2.1.2 Where the processing is necessary for taking steps at the request of the person to whom the data relates with a view to entering into a contract.

2.1.3 Where the processing is necessary to comply with any legal obligation (other than an obligation imposed by contract). This covers processing and disclosing information in realisation to employees of the HM Revenue and Customs and the Contributions Authority, to administer attachment of earnings orders and to deal with VAT accounting.

2.1.4 Where the processing is necessary to protect the vital interests of the person to whom the data relates. As the exact extent of this provision is unclear, and is viewed as extending only to extremely important issues such as the life and health of the person concerned, this provision must not be relied upon without express authority from the Data Protection Officer.

2.1.5 Where the processing is necessary for the purposes of legitimate interestspursued by S4C or by any third party to whom the data is disclosed. This condition is not available where the prejudice to the rights and freedoms or the legitimate interests of the person to whom the data relates is such that the law regards the processing as "unwarranted". This provision must not be relied upon without express authority from the Data Protection Officer.

2.2 **Additional Rules for Sensitive Personal Data**

When processing Sensitive Personal Data, if explicit written consent has not been obtained for the processing by the person to whom the data relates then one of the conditions outlined in paragraph 2.1 above must be fulfilled, together with one of the following requirements:

2.2.1 The processing is necessary for the purposes of exercising any right which is conferred by law on S4C or for the purposes of performing any obligation which is imposed by law on S4C in connection with employment. This covers processing for payroll and benefits purposes and also the issuing of Statements of Terms and Conditions of Employment.

2.2.2 The information contained in the data has been made public as a result of things done deliberately by the person to whom it relates. This might apply, for example, to someone who has made their political opinions or union membership public.

2.2.3 The processing is necessary for the purpose of, or in connection with, any legal cases or for the purposes of obtaining legal advice or otherwise dealing with legal rights. This provision must not be relied upon without express authority from the Data Protection Officer.

2.2.4 The processing is of information about racial or ethnic origin and is for the purposes of equal opportunity monitoring. This provision must not be relied upon without express authority from the Data Protection Officer.

2.3 General Rules for Consent

The requirements for obtaining and demonstrating consent can be demanding. In practice, you must not treat someone as having given consent unless you have identified that there is written consent which applies to the particular case.

3. MONITORING

You are required to comply at all times with the S4C Email and Internet Usage Policy (which can be found on the S4C intranet site) and use of email and the internet may be subject to monitoring by S4C from time to time for the purpose of checking that usage is in compliance with the Email and Internet Usage Policy.

Such monitoring will be undertaken in accordance with the DPA rules, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

4. CONCLUSION

S4C has a legal liability to ensure that personal data is processed in accordance with dataprotection legislation and principles. S4C cannot comply with its legal liability unless all employees ensure that they comply with this Rules and Guidance document. Employees and officers of S4C may also face criminal liability in certain circumstances for failure to comply with the DPA.

Data protection is a serious matter. A failure to comply with this Policy document will result in disciplinary action which could result in summary dismissal.

S4C provides compulsory data protection training which employees are required to attend.

If you want further information about data protection and the implications for you and S4C you should refer to the Data Protection Officer.