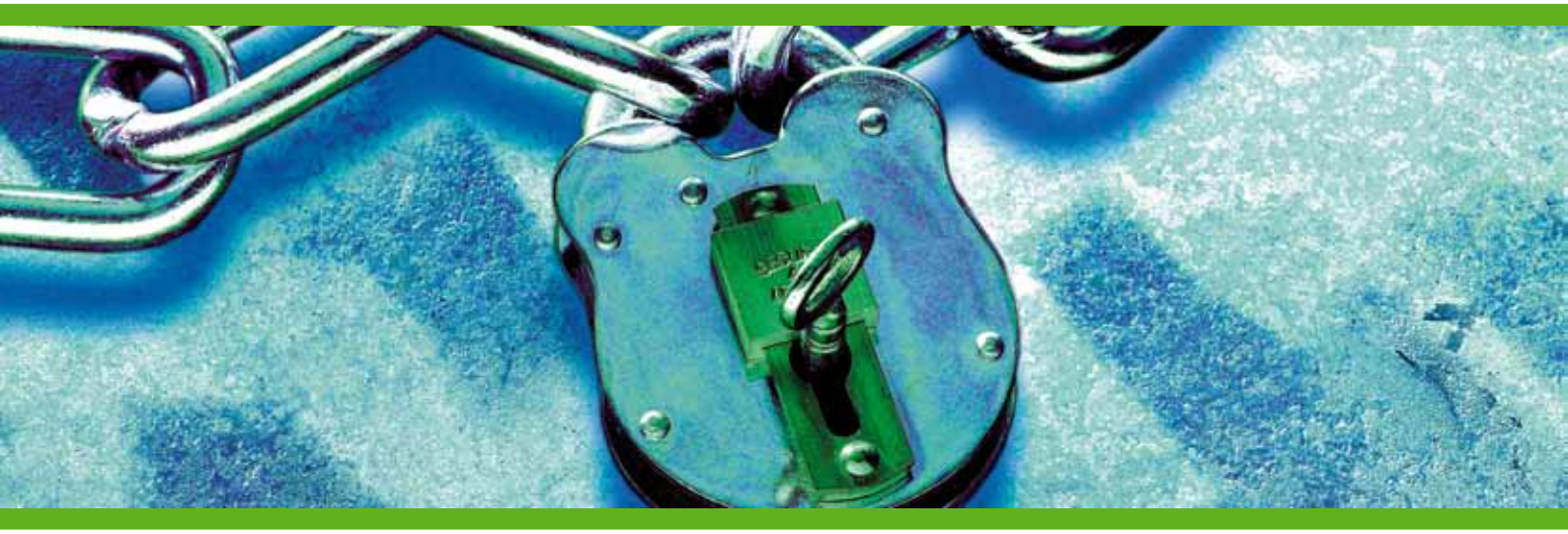
afbi Agri-Food and Biosciences Institute ®



AFBI DATA PROTECTION POLICY

POLICY STATEMENT OF THE AGRI-FOOD AND BIOSCIENCES INSTITUTE (AFBI)

www.afbini.gov.uk

AGRI-FOOD & BIOSCIENCES INSTITUTE (AFBI)

DATA PROTECTION POLICY

Reference:	AFBI POL 05/09
Date:	22 April 2009
Version:	2.0 (15 May 2018)
Author:	Governance & Performance Branch

Version Control

Version	April	
Version 1.1	August 2011	• Current post holder modified • Layout enhancements
Version 2.0	May 2018	• Updated to take account of GDPR/DPA 2018 and new roles/postholders

Table of Contents

INTRODUCTION 3

OBJECTIVES 4

POLICY STATEMENT 5

IMPLEMENTATION 9

CONCLUSION 11

GLOSSARY OF TERMS 12

APPENDIX 1 – AFBI Privacy Notice 13

APPENDIX 2 – Processing of Personal and Special Categories of Personal Data 18

INTRODUCTION

1. AFBI holds and processes a quantity of personal data which has been generated by our business over the years. Such data is held in a variety of formats, including computer records, structured and unstructured manual records, mobile devices, photographs, microfiches and on other media. It relates to both staff and members of the public and includes factual information (such as names, addresses and contact numbers) and opinions (such as staff reports).

2. While the Freedom of Information Act 2000 lays down provisions in relation to the disclosure of the majority of information held by AFBI, including personal information relating to third parties, it is the Data Protection Act 2018 that regulates how personal information relating to identifiable living individuals must be treated. The Data Protection Act 2018 is intended to protect personal privacy and to uphold the rights of individuals by regulating the processing of their personal information. It affords specific rights to individuals about whom personal information is held and places specific responsibilities upon those holding or processing that personal information.

3. The Data Protection Act 2018 takes into account the requirements of the EU General Data Protection Regulation (GDPR) which replaces Directive 95/46/EC of the European Parliament and Council. It will ensure a consistent and high level of protection of the rights and freedoms of EU citizens that is equivalent across the EU Member States and takes account of technological advances and globalisation since 1995.

4. The Freedom of Information Act 2000 came into operation on 1 January 2005 and brings all personal information under the scope of the UK Data Protection Act. This means that individuals are now entitled to use the Data Protection Act 2018 to request access to all personal information AFBI holds about them, whether it is held within a structured filing system or not.

5. As members of the public have grown more accustomed to the concept of freedom of information and become more familiar with their enhanced rights of access an increased number of information access requests involving personal information and a wider variety of data protection requests have been dealt with by AFBI. The Information Commissioner, who operates as an independent public official reporting directly to Parliament, has responsibility for ensuring that public authorities comply with the requirements of all information access legislation, including the Data Protection Act 2018, and has authority to take enforcement action against those which do not. It is important, therefore, that all staff in AFBI who hold or process personal information are familiar with the legislative requirements and the implications of this Data Protection Policy Statement.

OBJECTIVES

6. The objective of the Data Protection Policy Statement is to demonstrate AFBI's commitment to compliance with the Data Protection Act 2018,(incorporating the EU GDPR) and the Freedom of Information Act 2000, in relation to the following:

   - Quality: all personal data held by AFBI must be accurate and kept up to date;
   - Use: all personal data held by AFBI must be used only for the purpose or purposes for which it was collected;
   - Awareness: all staff whose work involves personal data must be fully aware of legal requirements relating to the holding and processing of this data;
   - Accountability: AFBI's Information Asset Owners must ensure that records are maintained demonstrating due consideration of the privacy–related risks associated with processing personal information within their business areas, e.g. Data Protection Impact Assessment (DPIA). Staff who deal with personal data should be personally responsible for their actions;
   - Confidence: everyone whose personal data is held by AFBI needs to be assured that their lives will not be affected adversely as a result of incorrect processing of their data; and
   - Respect: AFBI must fully respect the rights afforded to individuals under the Data Protection Act 2018 (incorporating EU GDPR) and provide clear, transparent information in the form of Privacy Notices.

   This Policy Statement sets out the guidelines for dealing with personal information and staff are directed towards the Data Protection section of the AFBI Intranet site for further guidance on the legislative requirements of the Data Protection Act 2018/GDPR.

POLICY STATEMENT

7. AFBI regards the fair, lawful and transparent treatment of personal information as a critical factor in the success of our operations and a key to the maintenance of the confidence that exists between those with whom we deal and ourselves. AFBI therefore acknowledges its legal obligations under the Data Protection Act 2018 (incorporating the EU GDPR) and endorses its provisions.

8. In order to carry out our duties, staff in many business areas need to collect and use specific information about people or groups of individuals. These include people who work for AFBI or have done so in the past, customers, suppliers, contractors and others. Such information must be managed properly regardless of how or why it is collected and irrespective of the format in which it is currently held. AFBI will take steps to ensure compliance with current and possible future legislation in the area of Data Protection.

9. In the case of personal information relating to current members of staff, HR Connect now requires members of staff to input their own personal data. Each member of staff is responsible for the accuracy of his/her own personal data and for compliance with AFBI's obligations in this regard.

10. The Data Protection Act 2018 is centred around the following six Data Protection Principles and AFBI will ensure through appropriate management and the strict application of controls that it complies with these:

    - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
    - personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes; further processing for scientific research or statistical purposes shall, in accordance with Article 89(1) of GDPR, not be considered to be incompatible with the initial purposes (it should be made clear at the time of collection that the data being collected may be used in such ways);
    - personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
    - personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for that purpose; however, personal data may be held for longer periods for scientific research or statistical purposes in accordance with Article 89(1) of the GDPR subject to required appropriate technical and

organisational measures to safeguard the rights and freedoms of the data subject.

- personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, damage or destruction of that data, using appropriate technical or organisational measures;

11. The Data Protection Act also affords a number of rights to those about whom we hold personal information (data subjects). AFBI acknowledges these rights and is committed to respecting and safeguarding them in the way in which it holds and processes personal data. The specific rights given to data subjects are as follows:

- the right to know if AFBI is processing personal data relating to them as individuals and to request a copy of that data and specified associated information, such as details of the source of the data or any recipients of same or the length of time the data will be held(such requests must be dealt with within the 1 month legislative deadline). As noted in paragraph 1, opinions are covered by the Data Protection Act and so are disclosable under a subject access request – in view of this, it is recommended that subjective or personal opinions about a named individual are recorded only with good reason;
- the right to object to or prevent processing of personal data in certain circumstances;
- the right to not be subject to a decision based solely on automated processing if it is likely to significantly affect the data subject;
- the right to compensation, payable by AFBI, for damage and distress we cause the data subject by any contravention of the Act;
- the right to require AFBI, in certain circumstances, to rectify, restrict the use of, erase or provide personal data in a portable machine-readable format; and
- the right to ask the Information Commissioner to assess whether or not it is likely that any processing of personal data has been or is being carried out in contravention of the Act.

12. In order to uphold these rights of data subjects AFBI will ensure that:

- there is a Data Protection Officer (DPO) appointed with specific responsibility for data protection - this is currently Glenn Montgomery, Head of Governance & Performance Branch, (FCAD), Ext 55494;
- Heads of Branch are assigned as Information Asset Owners (IAO) with oversight by the Senior Information Risk Owner (SIRO) to provide assurance on the compliance with DPA within their business areas;

- everyone processing personal information is appropriately trained and supervised, and that they understand that they are directly and personally responsible for following good data protection practice;
- queries about processing personal information are dealt with promptly and courteously using an established and legally compliant procedure (e.g. Subject Access Request);
- methods of processing personal information are described clearly in relevant Privacy Notices and evaluated regularly; and
- actual performance in the processing of personal information is assessed regularly.

13. AFBI's Privacy Notice (Appendix 1) provides a useful summary of how AFBI is entitled to use or process the personal information it holds. This is published on AFBI's website and a link either to it or a more specific Privacy Notice should be incorporated into all forms used by AFBI for the collection of personal information so that data subjects know how AFBI proposes to process their personal details. This enables business areas to share personal data between each other in line with the Data Protection Act 2018 and Freedom of Information legislation. Personal information which is not collected under a Privacy Notice may normally be used only for the purpose(s) for which it is collected, which places automatic limitations on how it can be shared across AFBI – data subjects are entitled to be informed at the time personal information is collected how it will be used and any wider use is in contravention of the Data Protection Act. It is particularly important to note this at a time when developments in mobile computing and information technology have made the potential for the easy transfer of information so much greater than it was in the past.

14. The sharing of bulk personal information to enable another public body to trawl through it for its own purposes is prohibited by the Data Protection Act. This does not mean that AFBI will not provide personal information to other organisations when required to do so in order to facilitate, for example, fraud or criminal investigations – under these circumstances AFBI will provide specific information about an individual or number of individuals under investigation as distinct from bulk personal information about a particular class of data subjects (e.g. farmers or employees), except in circumstances where the organisation has specific statutory powers to request such information. Any business area receiving requests for personal information of this type should consult the DPO before taking any other action. A Data Sharing Agreement must be in place for any instances of sharing personal information between AFBI and a third party organisation.

15. Sharing of personal data between AFBI and any organisation outside of the European Economic Area (EEA) must be approved by the AFBI DPO to ensure it will be subject to the same level of data protection safeguards experienced within the EEA.

16. Some of the personal data which AFBI holds falls into special categories of personal data. These include information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information and sex life or sexual orientation.. Requirements for the processing of such categories of personal data are more onerous than those for other personal information – the normal requirements for the processing of personal data are outlined in Article 6 of the GDPR and the additional requirements relating to sensitive personal information are detailed in Article 9. A summary of the list of the requirements of both Articles is attached at Appendix 2. AFBI will ensure that any sensitive personal data it holds is processed in accordance with these requirements.

17. It has been apparent since January 2005 that third parties often submit Freedom of Information requests involving the personal information of members of staff or others. Whenever this happens AFBI is committed to ensuring that the six Data Protection Principles outlined in paragraph 10 are applied fairly and that all legislative requirements intended to safeguard the personal information of data subjects are met.

18. It is extremely important that AFBI is able to demonstrate that it takes adequate steps to safeguard the personal data and special categories of personal data it processes and this applies equally when it is being processed by others on AFBI's behalf (as with HR Connect for example). Under these circumstances the processing organisation must provide guarantees about the security of the processing being done for AFBI and these guarantees must be in the form of a written contract. Security measures must be at least equivalent to those we would apply if doing the job ourselves. If any security breach involving personal data occurs this must be reported to the AFBI DPO at once.

19. As a holder of personal information (data controller) AFBI is legally obliged to maintain a record of processing activities under its responsibility. This record will comprise of AFBI's Information Asset Register, Retention & Disposal Schedule and over-arching AFBI Privacy Notice and will be made available to the UK Information Commissioner upon request. Business areas must ensure to regularly review their Branch Information Asset Register and inform the DPO as and when an amendment is required throughout the year.

IMPLEMENTATION

20. Responsibility for delivering the actions outlined in paragraph 11 rests with both Governance & Performance Branch (GPB) and business areas. GPB plays a central role in terms of raising awareness, provision of advice and the instigation of investigations into any complaint. However, it is the responsibility of AFBI's IAOs (Heads of Branch) to review procedures, to monitor performance and to satisfy themselves that all members of staff who deal with personal information are fully aware of their responsibilities and follow correct procedures to ensure compliance with the Data Protection Act 2018 and GDPR. IAOs are responsible and accountable for the information held and processed within their business area and must give assurance regularly to the AFBI SIRO.

21. Specific actions to be taken by GPB include:

- making available to business areas the information they require to comply with the legislation – this will include publicising this policy, putting information on the intranet, ensuring adequate training is available, liaising with business areas, responding to queries from business areas and inputting to induction procedures;
- confirming with business areas on an annual basis that they are content with the data processing procedures they have in place;
- coordination of the annual review of AFBI's Information Asset Register and Privacy Notice;
- maintaining a central log of Data Protection Impact Assessments and Data Sharing Agreements;
- following the report of a personal data incident or breach, ensuring the correct implementation of the AFBI Data Breach Management Plan; and
- instigation of complaint investigations.

22. Specific actions to be taken by business areas include:

- ensuring relevant staff attend appropriate training courses and are familiar with the requirements of the Data Protection Act 2018 and GDPRand that necessary procedures are in place and followed;
- ensuring all personal information is accessible in the event that it is requested by a data subject;
- ensuring requests for personal information are dealt with within the legislative deadline;
- ensuring that personal information is kept secure, is accessible only to those who need to process it for approved purposes, and is only transferred to other organisations or disposed of appropriately in accordance with AFBI's procedures and the provisions of the Data Protection Act 2018 (incorporating the EU GDPR). Advice on when it

is appropriate to use techniques like encryption should be sought from AFBI's IT Security Officer or DPO;

- reporting any breach of personal data security to the AFBI DPO at once (following the AFBI Data Breach Management Plan);
- ensuring that data protection issues are considered and are documented (for example, in Data Protection Impact Assessments & Privacy Notices);
- reviewing internal procedures annually;
- liaising with GPB about any data protection issue they are unsure about.

The Information Asset Owner (Head of Branch) within each business area has specific responsibility for ensuring these aspects are taken forward.

CONCLUSION

23. Under this Data Protection Policy, which has been endorsed by the AFBI Executive Management Team and Board, overall responsibility for compliance with the provisions of the Data Protection Act 2018 and EU GDPR rests with the AFBI Chief Executive. In practice, however, many of the functions are devolved to the Senior Information Risk Owner (SIRO, Head of Finance & Corporate Affairs Division) and Data Protection Officer (DPO, Head of Governance & Performance) who are expected to oversee compliance in conjunction with IAOs. The DPO and Information Governance & Records Manager in GPB are available to advise on issues which arise. All staff who process personal information, should ensure that their job descriptions and, if necessary, their Personal Development Plans and Personal Performance Agreements, include these responsibilities.

24. AFBI will review its procedures regularly to ensure continued compliance with this Policy Statement which, itself, will be reviewed by GPB at three-yearly intervals.

GLOSSARY OF TERMS

Data – recorded information whether stored electronically, on a computer, or on certain paper-based filing systems.

Data Controller – a person or organisation, like AFBI, holding/using personal data and determining how and why information is processed. As a data controller an employer has a responsibility to establish workplace practices and policies that comply with the Data Protection Act 2018 and GDPR.

Data Subject – an individual to whom personal information relates; within the workplace a data subject may be a current or former employee or someone applying for a job but a data subject could also be a customer, client, supplier or indeed anyone about whom personal information is held.

Privacy Notice – a statement of how AFBI may process personal information. The Privacy Notice is to be published on the AFBI website and a weblink included on all forms used for the collection of personal information.

Information Commissioner – this is an independent public official reporting directly to Parliament.

Personal Data/Information – any information relating ***directly or indirectly*** to an identified or identifiable living individual; it can be factual or an opinion. It is important that the information has the data subject as its focus and affects the individual's privacy in some way.

Processing – this is any activity that involves personal data, including collecting, recording, structuring, retrieving, consulting, holding, disclosing or using it; also doing work on the data such as organising, adapting, changing, erasing or destroying it. The Data Protection Act 201 and EU GDPR requires that personal data be processed lawfully, fairly and transparently so data controllers have to meet certain conditions. A data subject must be told the identity of the data controller and why his or her personal information is being or will be processed.

Processing Personal Data – this can be done only where at least one of the conditions set out in Article 6 of the EU GDPR has been met (see Appendix 2).

Processing Special Categories of Personal Data – this can be done only where at least one of the conditions set out in Article 9 of the GDPR (see Appendix 2).

Special Categories of Personal Data –includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, and sex life or sexual orientation.

APPENDIX 1 – AFBI Privacy Notice

AFBI Privacy Notice

Data Controller Name: Agri-Food & Biosciences Institute Address: 18a Newforge Lane Telephone: 02890 255636 Email: info@afbini.gov.uk	Data Protection Officer Name: Head of Governance & Performance Telephone: 028 9025 5494 Email: foi.officer@afbini.gov.uk

Why are you processing my personal information?

We process personal information to perform our services; maintain our accounts and records and to support and manage our employees.

The lawful basis for processing is normally either based on:

(i) a contract e.g. employee contract, commercial contract, funding award contract; or
(ii) the performance of a public task.

The Institute has the authority to process personal information for the completion of its public task function of undertaking scientific work as legislated under The Agriculture (Northern Ireland) Order 2004 in the fields of:

- agriculture;
- animal health & welfare;
- food;
- fisheries;
- forestry;
- the nature environment; and
- rural development and enterprise.

The term “scientific work” includes:

- Research and development;
- The testing or analysis of any matter;
- The provision of advice and information on scientific matters; and
- The dissemination or application of the results of scientific research.

AFBI may use samples submitted for diagnostic testing for further disease surveillance or research work. This includes looking for new or emerging diseases and monitoring changes in disease or infectious agents.

As a publicly funded body, the Institute is under a duty to protect the public funds it administers and to this end may use the information you have provided for this purpose.

In exceptional circumstances, the Institute may rely on

(iii) your consent to collect and process your personal information.

If this is the case, you will be fully informed of the reasons for processing and will be given the opportunity to provide freely given, specific and informed consent and will be provided with information on its withdrawal.

What categories of personal data are you processing?

We process personal information about:

- our clients
- our employees
- enquirers, complainants
- consultants and professional advisors
- suppliers and service providers

We process information relevant to the above reasons/purposes. This may include:

- personal details, e.g. name, address, telephone number, herd number
- family details
- lifestyle and social circumstances
- education and employment details
- financial details
- goods or services provided

We also process sensitive classes of information that may include:

- race or ethnic origin
- religious or other beliefs
- trade union membership
- physical or mental health details

Where do you get my personal data from?

Personal data may be obtained from a variety of public bodies and private sources: e.g. Government Departments such as the Department of Agriculture, Environment and Rural Affairs (DAERA); Private Veterinary Practitioners, Occupational Health Service and third party processors/suppliers. Information may also be collected directly from the individual.

AFBI uses Closed Circuit Television (CCTV) systems for maintaining the security of property and premises and for preventing and investigating crime; it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where appropriate and necessary, this information is shared with the individuals recorded, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

Do you share my personal data with anyone else?

We may share your information with other bodies responsible for the audit or administration of public funds, in order to prevent and detect fraud. We may also share information with the Police Service Northern Ireland (PSNI) and other crime agencies for the prevention or detection of crime.

As a public body, we are obliged to comply with information requests under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 where such disclosure is in the public interest, but shall always ensure your rights under UK Data Protection legislation are respected.

Where necessary or required we share information with:

- you, (responding to a subject access request)
- family, associates and representatives of the person whose personal data we are processing
- current, past or prospective employers
- internal and external auditors
- educators and examination organisations
- financial organisations
- employment and recruitment agencies
- credit reference agencies
- debt collection and tracing agencies
- research organisations
- government departments e.g. Department for Agriculture, Environment & Rural Affairs (DAERA)
- PSNI or other crime agencies
- business associates
- suppliers and service providers

Do you transfer my personal data to other countries?

Sometimes it may be necessary to transfer personal information overseas to share with partner research organisations. When this is necessary, information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the UK Data Protection legislation and the EU General Data Protection Regulation.

How long do you keep my personal data?

We will retain your data for as long as necessary to fulfil the purpose for which it was gathered and, unless required to be held long-term for scientific research or statistical purposes, it will be held by AFBI for no longer than stipulated by legislation, or to a maximum of 20 years.

[TO REPLACE THE PARAGRAPH ABOVE WHEN AFBI'S R&D SCHEDULE IS APPROVED BY NI ASSEMBLY…..We will only retain your data for as long as necessary to fulfil the purpose and in line with our Retention and Disposal Schedule (*Provide a hyperlink to the AFBI R & D once published on AFBI website)*].

Under the UK Data Protection Act 2018, AFBI is allowed to hold your personal information long-term if required for scientific research or statistical purposes. If this is the case, we will ensure that the appropriate technical and organisational measures are in place to safeguard your data where necessary and respect the principle of data minimisation.

What rights do I have?

- You have the right to obtain confirmation that your data is being processed, and access to your personal data
- You are entitled to have personal data rectified if it is inaccurate or incomplete
- You have a right to have personal data erased and to prevent processing, in specific circumstances
- You have the right to 'block' or suppress processing of personal data, in specific circumstances
- You have the right to data portability, in specific circumstances
- You have the right to object to the processing, in specific circumstances
- You have rights in relation to automated decision making and profiling

How do I complain if I am not happy?

If you are unhappy with any aspect of this privacy notice, or how your personal information is being processed, please contact AFBI's Data Protection Officer at*:*

AFBI HQ, 18a Newforge Lane, Belfast, BT9 5PX;

foi.officer@afbini.gov.uk

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Email: casework@ico.org.uk

https://ico.org.uk/global/contact-us/

Other websites

Our website may contain links to other websites. This privacy policy only applies to this website so when you link to other websites you should read their privacy policies.

APPENDIX 2 – Processing of Personal and Special Categories of Personal Data

This is an indicative summary – for more detail please refer directly to the EU General Data Protection Regulation.

Processing of personal data can only be carried out where at least one of the following lawful conditions set out in Article 6 of the EU GDPR has been met. Processing must be:

- with the consent of the data subject;
- necessary for the performance of a contract with the data subject;
- for the compliance with any legal obligation (other than contractual);
- to protect the vital interests of the data subject;
- to carry out public task functions; or
- to pursue legitimate interests of the data controller except where such interests are overridden by the rights and freedoms of the data subject. *N.B. this condition does not apply to interests pursued by public authorities in relation to their public task function.*

To process special categories of personal data at least one of the conditions set out in Article 9 of the EU GDPR must be met. Processing must be:

- with the explicit consent of the data subject;
- necessary to comply with the data controller's legal duty in connection with employment;
- to protect the vital interests of the data subject or another person;
- carried out by certain non-profit bodies;
- where the information has been made public by the data subject;
- in legal proceedings, to obtain legal advice, or exercise legal rights;
- to carry out public functions;
- for medical purposes;
- for equality opportunities monitoring; or
- for archiving in the public interest or for scientific or historical research or statistical purposes.