

**AGRI-FOOD
& BIOSCIENCES
INSTITUTE**

Data Protection Policy
November 2020, version 3.0

DATA PROTECTION POLICY

Guidance for AFBI staff in dealing with the personal information of colleagues, customers and other stakeholders.

Document Information

Reference	AFBI POL 05/09	
Author:	Governance and Performance Branch	
Approval:	AFBI Board on 22 April 2009 (version 1.0) AFBI Board on 15 May 2018 (version 2.0) AFBI Board on 26 Nov 2020 (version 3.0)	
Version	Date of issue	Reason for issue
Version 1.0	April 2009	First issue of policy
Version 1.1	Aug 2011	Current post holder modified Layout enhancements
Version 2.0	May 2018	Updated to take account of GDPR/DPA 2018 and new roles/postholders
Version 3.0	Nov 2020	Triennial review, incorporating internal audit recommendations

Contents

1	Purpose of this document	1
2	Audience.....	1
3	Introduction	2
4	AFBI's data protection commitments	3
5	Data protection principles	3
6	Data subjects' rights	7
7	Lawful bases for processing personal data, including special categories of personal data.....	8
8	Privacy notices.....	8
9	Data Protection Impact Assessments	9
10	Sharing of personal data with UK organisations	9
11	International transfers of personal data	10
12	Requests for disclosure of personal data.....	10
13	Processing by third parties	10
14	Documentation and record-keeping.....	11
15	Security of data	11
16	Implementation of policy.....	12
17	Compliance with policy	13
18	Monitoring and Review	13
	APPENDIX 1: Associated policies and procedures.....	i
	APPENDIX 2: Lawful bases for processing personal information.....	ii
	APPENDIX 3: AFBI privacy notice template	v
	APPENDIX 4: Glossary of Terms	viii

1 Purpose of this document

This document offers guidance for AFBI staff in dealing with the personal information of colleagues, customers and other stakeholders, and demonstrates AFBI's commitment to compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)¹ – as well as the Freedom of Information Act 2000, in relation to:

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	•Staff who deal with personal data should be personally responsible for their actions; Information Asset Owners are responsible for maintaining evidential records for their business area
Confidence	•everyone whose personal data is held by AFBI needs to be assured that their lives will not be adversely affected as a result of incorrect processing of their data
Respect	•AFBI must fully respect the rights afforded to individuals under UK Data Protection legislation and provide clear, transparent information in the form of privacy notices

Staff are directed towards the [data protection section of the AFBI intranet](#)² site for further guidance on the legislative requirements of the Data Protection Act 2018 and the GDPR.

2 Audience

This policy statement and the procedures associated with it (see [Appendix 1](#) on associated policies and procedures) are aimed at all AFBI staff and stakeholders.

¹ See https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en for GDPR legal text

² See <http://afbi.intranet.nigov.net/data-protection>. Readers without access to the AFBI intranet should contact AFBI's Information Governance Unit at info.gov@afbini.gov.uk

3 Introduction

AFBI holds and processes a quantity of personal data which has been generated by our business over the years.

Personal data is defined in the GDPR as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Such data are held in a variety of formats, including computer records, structured and unstructured manual records, mobile devices, photographs, microfiches and on other media. They relate to both staff and members of the public and include factual information (such as names, addresses and contact numbers) and opinions (such as staff reports).

While the Freedom of Information Act 2000 (FOIA) 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 (DPA) that regulates how personal information relating to identifiable living individuals must be treated. The DPA 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. The DPA takes into account the requirements of the GDPR.

The FOIA came into operation on 1 January 2005 and brings all personal information under the scope of the DPA. This means that individuals are entitled to use the DPA to request access to all personal information AFBI holds about them, whether it is held within a structured filing system or not.

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, 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 DPA, 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.

4 AFBI's data protection commitments

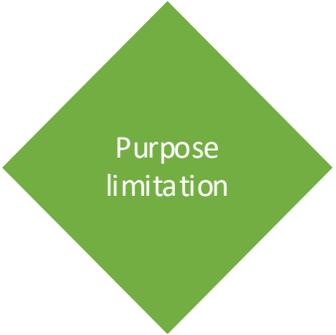
AFBI regards the fair, lawful and transparent treatment of personal information as a critical factor in the success of our operations and a key to the maintenance of the confidence that exists between those with whom we deal and ourselves. AFBI therefore acknowledges its legal obligations under the DPA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

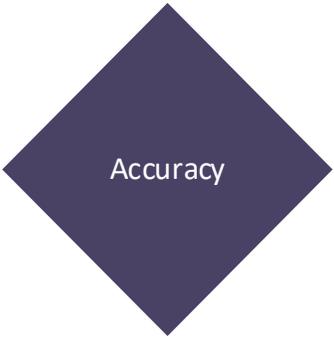
In order to carry out our duties, staff in many business areas need to collect and use specific information about people or groups of individuals. These include people who work for AFBI or have done so in the past, customers, suppliers, contractors and others. Such information must be managed properly 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.

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.

5 Data protection principles

The legislative framework described above is founded on seven data protection principles and AFBI will ensure through appropriate management and the strict application of controls that it complies with these. The principles, and their specific application to AFBI are set out in Table 1.

Data protection principle	What the GDPR says	What it means for AFBI
 <p>Lawfulness, fairness and transparency</p>	<p><i>'Personal data will be processed lawfully, fairly and in a transparent manner in relation to individuals.'</i></p>	<p>AFBI teams need to ensure that staff and customers can understand what it is they are signing up to when they hand over their personal data. This principle requires that we use language that is 'clear, plain and accurate' as to what a data subject is consenting to, thus helping to ensure the data rights and legal protections.</p> <p>In practice, AFBI business areas and their information asset owners should ensure – if necessary by carrying out a data protection impact assessment or DPIA – that any processing of personal data has a basis in law as defined by Article 6 of the GDPR, and is accompanied by an appropriate privacy notice.</p> <p>In most cases, the processing of personal information by AFBI business areas will be based on AFBI's 'public task', the consent of the individual data subject, or contractual necessity. (See appendix 2 for more details of the available legal bases for the processing of personal data.)</p>
 <p>Purpose limitation</p>	<p><i>'Personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.'</i></p>	<p>Any personal data collected by AFBI for a specific, previously stated and understood purpose, must not then be used for another purpose.</p> <p>Though the GDPR states that this principle of purpose limitation is not incompatible with processing for public interest or scientific or statistical purposes, it does mean that AFBI teams need to consider very carefully any proposal to 'multi-purpose' personal data (and consult the data protection officer.)</p>

Data protection principle	What the GDPR says	What it means for AFBI
 <p data-bbox="293 373 465 437">Data minimisation</p>	<p data-bbox="600 236 1252 339"><i>'Personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.'</i></p>	<p data-bbox="1274 236 2011 376">AFBI business areas and their information asset owners need to ensure that the extent or amount of data collected and/or processed is adequate, relevant and limited to the intended purpose.</p> <p data-bbox="1274 419 2022 560">AFBI teams should not 'hoard' data without a clear rationale and should limit the personal data collected to that necessary to achieve the specific purpose in mind – not a 'just in case' approach.</p>
 <p data-bbox="320 756 439 788">Accuracy</p>	<p data-bbox="600 603 1232 778"><i>'Personal data will 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.'</i></p>	<p data-bbox="1274 603 1939 707">When storing personal data, business areas and their information asset owners are responsible for either updating inaccurate information or getting rid of it.</p>
 <p data-bbox="315 1131 443 1195">Storage limitation</p>	<p data-bbox="600 962 1249 1353"><i>'Personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.'</i></p>	<p data-bbox="1274 962 1939 1066">The principle of storage limitation prevents AFBI from keeping hold of data for indefinite periods of time, or beyond that of its intended purpose.</p> <p data-bbox="1274 1109 2022 1321">Again, purposes of public interest, archiving, and scientific research or statistics may act as reasons for an organisation retaining personal data, but these reasons <u>must</u> be justifiable and documented. The data protection officer should be consulted where business areas propose to retain personal data for these purposes.</p>

Data protection principle	What the GDPR says	What it means for AFBI
 <p data-bbox="280 363 461 432">Integrity and confidentiality</p>	<p data-bbox="600 236 1245 448"><i>'Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'</i></p>	<p data-bbox="1274 236 2007 411">The integrity and confidentiality of personal data must be upheld with the appropriate security measures. Business areas and their information asset owners must implement appropriate physical and technological controls and follow any relevant IT and physical security policies and guidance.</p>
 <p data-bbox="280 713 461 750">Accountability</p>	<p data-bbox="600 569 1234 635"><i>'The controller shall be responsible for, and be able to demonstrate compliance with, [these principles.]'</i></p>	<p data-bbox="1274 569 2018 708">AFBI's Executive Management Team and senior information risk owner take responsibility for any personal data being handled by the institute, and for its compliance with the other six principles.</p> <p data-bbox="1274 751 2002 855">AFBI business areas and their information asset owners must ensure that the required processes are documented and appropriate records kept to demonstrate compliance.</p>

Table 1: The data protection principles and what they mean for AFBI

6 Data subjects' rights

The DPA also affords a number of rights to those about whom we hold personal information (known as '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:

Right to be informed	Right to request access	Right to rectification	Right to erasure ("Right to be forgotten")
Right to restrict processing	Right to data portability	Right to object or withdraw consent	Rights regarding automated decision-making
Right to be informed of a personal data breach	Right to lodge a complaint	Right to compensation	Right to representation

Further information on these rights are available in our "Citizen's Guide to GDPR – What are my rights?" publication³ on the AFBI website.

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, Ext 55494;
- Heads of Branch are assigned as Information Asset Owners (IAOs) 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. the subject access request procedure described in section 10 below);

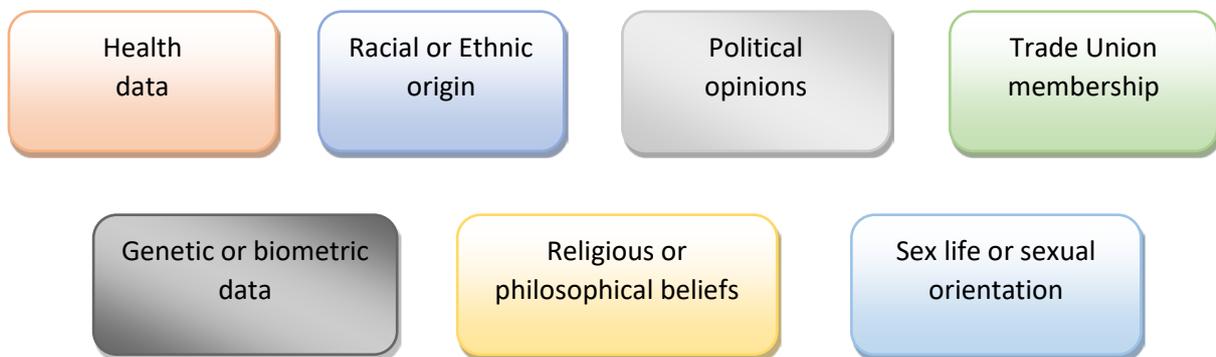
³ <https://www.afbini.gov.uk/publications/afbi-guide-citizens-rights-under-gdprdata-protection-act-2018>

- 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.

7 Lawful bases for processing personal data, including special categories of personal data

AFBI must have a valid lawful basis for processing personal data; there are six available under Article 6 of the GDPR and the most appropriate will depend on the purpose and relationship with the individual.

Some of the personal data which AFBI holds may fall into special categories of personal data, also known as 'sensitive personal data'. These may include information about an individual's:



The lawful bases for the processing of such special categories of personal data are more restricted than those available for other personal information and an additional lawful basis must be identified from Article 9 of the GDPR before any sensitive personal data can be processed.

A summary of the available lawful bases set out in both articles is attached at [Appendix 2](#), along with relevant examples to aid AFBI staff when coming to a decision on which lawful basis is the most appropriate to apply. AFBI will ensure that any personal and sensitive personal data it holds is processed in accordance with these requirements.

8 Privacy notices

The Institute's Privacy Notice⁴ published on AFBI's website provides an overarching guide to how AFBI is entitled to use or process the personal information it holds. For more task-specific occasions, for example a particular scientific project or service, staff should use the Privacy Notice template ([Appendix 3](#)) available on the

⁴ <https://www.afbini.gov.uk/afbi-privacy-notice>

Intranet and consult the Data Protection Officer for advice. A link either to the Institute privacy notice or a more specific privacy notice will be available as part of any exercise where AFBI collects or otherwise processes personal information, so that data subjects know how AFBI proposes to process their personal details.

9 Data Protection Impact Assessments

The General Data Protection Regulation introduces a requirement to complete a Data Protection Impact Assessment before carrying out any types of processing likely to result in high risk to individuals' interests.

A Data Protection Impact Assessment screening exercise is a process to help business areas make an initial evaluation of the probable level of risk involved in their planned process and therefore minimise the data protection risks of any project. Should the screening exercise indicate a higher risk process being undertaken, it is now a statutory requirement that a full Data Protection Impact Assessment must be undertaken before further development of the process can proceed.

Business areas should follow the DPIA guidance available on the intranet and in particular undertake screening exercises at an earliest stage possible.

If a Data Protection Impact Assessment identifies a high risk that a business area cannot mitigate, staff must consult with AFBI's Data Protection Officer who will provide advice. The Data Protection Officer may need to consult with the ICO who will provide written advice. This advice can take up to 14 weeks and this timeline reinforces the need for the timely carrying out of Data Protection Impact Assessment's.

10 Sharing of personal data with UK organisations

The Institute will provide personal information to another public body or external organisation where there is a legitimate and lawful reason for doing so, including to auditors, research collaborators and funding bodies.

Sometimes the Institute is required to provide personal information 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. Any potential for personal data to be shared will be made clear in privacy notices produced by AFBI business areas.

11 International transfers of personal data

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 provided by the GDPR. Business areas and project teams who transfer personal data to, or receive personal data from, individuals or organisations based outside the EEA, will ensure that such processing is accompanied by appropriate legal safeguards, for example the integration of specific clauses into the contract governing a partnership which guarantee the legal rights of data subjects.

Following the exit of the United Kingdom from the European Union, business areas and project teams sharing personal data with partners within the EEA may require similar safeguards. Affected business areas should seek the advice of AFBI's DPO.

12 Requests for disclosure of personal data

The DPA and the GDPR give individuals the right to be told what information AFBI holds about them and, unless an exemption applies, to receive a copy of that information. They do this by making a data subject access request or SAR.

The request may be in writing (including faxes and emails) or verbally. If a request is made by telephone or in person, it should be recorded in an email and sent to foi.officer@afbini.gov.uk. All written requests should also be sent to this address for recording.

To ensure that all staff can recognise a SAR and treat it appropriately, AFBI has produced a [subject access request procedure manual](#) that is available to staff on the AFBI intranet⁵.

Third parties often submit environmental or freedom of information requests involving the personal information of members of staff or others. Whenever this happens AFBI is committed to ensuring that the data protection principles described in Table 1 are applied fairly and that all legislative requirements intended to safeguard the personal information of data subjects are met.

13 Processing by third parties

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.

⁵ See <http://afbi.intranet.nigov.net/publications/data-protection-act-2018-subject-access-request-procedure-manual>. Readers without access to the AFBI intranet should contact AFBI's Information Governance Unit at info.gov@afbini.gov.uk

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 or equivalent. Security measures must be at least comparable 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.

14 Documentation and record-keeping

As a holder and decision-maker 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 and over-arching AFBI Privacy Notice and will be made available to the Information Commissioner upon request. Business areas must ensure to regularly review their entries in the Information Asset Register and the DPO will have an oversight role to ensure the quality of the information contained within.

15 Security of data

Business areas, their IAOs, and individual members of AFBI staff are responsible for ensuring compliance with the Institute's physical and electronic security policies and guidance. In particular, AFBI's [Information Security Policy](#), the NICS-wide [IT Security - NICS Guide to Physical, Document & IT Security](#), the [IT Guidelines - GDPR](#) guidance document, and the [Mobile Device Security Policy \(NICS\)](#)⁶.

In the event of any breach involving personal data which is likely to result in a risk to the rights and freedoms of individuals, this must be reported to the DPO **as soon as possible** as the DPO must report it to the Information Commissioner within 72 hours of the Institute being aware of it (not from when it has been reported to the DPO). Business areas should ensure that they act in accordance with the [AFBI Data Breach Management Plan](#).

The Institute will act in accordance with the Information Commissioner's advice on the four elements of a breach management plan which are:-

- Containment and recovery;
- Assessment of ongoing risk;
- Notification of breach;
- Evaluation and response.

⁶ Links to these and other relevant policies can be found in Appendix 1. Readers without access to the AFBI intranet should contact AFBI's Information Governance Unit at info.gov@afbini.gov.uk

16 Implementation of policy

Responsibility for delivering the actions outlined in the preceding paragraphs rests with both the Governance & Performance Branch (GPB) and individual 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 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 DPA 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.

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 regular reviews of the institute's over-arching privacy notice;
- maintaining a central log of data protection impact assessments and data sharing agreements;
- ensuring the appropriate data protection fee is paid to the Information Commissioner's Office within the required timeframes;
- following the report of a personal data incident or breach, ensuring the correct implementation of the AFBI [Data Breach Management Plan](#)⁷; and
- instigation of complaint investigations.

Specific actions to be taken by business areas include:

- ensuring relevant staff attend appropriate training courses and are familiar with the requirements of the DPA and GDPR and that necessary procedures are in place and followed;

⁷ Available to AFBI staff on the institute's intranet site at <http://afbi.intranet.nigov.net/publications/data-breach-management-plan>. Readers without access to the AFBI intranet should contact AFBI's Information Governance Unit at info.gov@afbini.gov.uk

- 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 DPA and GDPR. Advice on the appropriate use of 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 and privacy notices);
- reviewing internal procedures annually;
- liaising with GPB about any data protection issue they are unsure about.

The IAO within each business area has specific responsibility for ensuring these aspects are taken forward.

17 Compliance with policy

Under this policy, which has been endorsed by the AFBI Executive Management Team and Board, overall responsibility for compliance with the provisions of the DPA and 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.

Failure to comply with the provisions of this policy may result in appropriate disciplinary action being taken.

18 Monitoring and Review

This data protection policy statement and its associated documentation will be reviewed by AFBI's Information Governance Unit on a regular basis, and at least

every three years, or following significant changes to relevant legislation or best practice standards.

APPENDIX 1: Associated policies and procedures

AFBI staff are contractually obliged to comply with a range of policies and procedural guidance documents published on the AFBI Intranet which have a bearing on how personal data is collected, processed, stored and ultimately disposed of. These include:

- [Clear Desk & Screen Policy](#)
- [Data Protection - Guidance and Link to legislation](#)
- [Data Protection Act 2018 - Subject Access Request Procedure Manual](#)
- [Data Protection/GDPR - Conducting a Legitimate Interests Assessment](#)
- [Data Breach Management Plan](#)
- [Data Sharing Guidance](#)
- [Electronic Communications - Good practice guidance](#)
- [Encryption of External Communications Policy](#)
- [Freedom of Information](#)
- [Information Security Policy](#)
- [IT Security - NICS Guide to Physical, Document & IT Security](#)
- [IT Guidelines - GDPR](#)
- [Mobile Device Security Policy \(NICS\)](#)
- [Records Management Policy](#)
- [Retention and disposal schedule](#)
- [Travelling with mobile IT devices - Guidance](#)
- [Use of Cloud-based Shared Services - Guidance](#)
- [Video Conferences \(recording of\) - NICS Policy](#)

Readers without access to the AFBI intranet should contact AFBI's Information Governance Unit at info.gov@afbini.gov.uk.

APPENDIX 2: Lawful bases for processing personal information

Under the General Data Protection Regulations (GDPR) and UK Data Protection Act 2018, you must have a lawful basis in order to process the personal data of living individuals. The GDPR offers six bases that AFBI, as a public authority, can normally choose from to rely on for processing personal information. These are set out in the table below.

Lawful basis in GDPR	Illustrations or examples of potential use in AFBI processing
Article 6(1)(a): Consent has been given by the individual.	Where a survey participant actively consents to receive further communications from the project team.
Article 6(1)(b): Necessary under a contract with the individual,	<p>Where it is necessary for AFBI to process the personal data of another party to enter into a contract to supply goods or services to that party, or to establish and manage a partnership agreement or service level agreement with them.</p> <p>For HR staff processing the personal data of AFBI employees this is likely to be the most usual lawful basis under GDPR.</p>
Article 6(1)(c): Compliance with a legal obligation, i.e. where you are required by UK or EU law to process the data for a particular purpose.	Where it is necessary to process someone's personal information to comply with health and safety legislation, or with legislation in the field of employment law
Article 6(1)(d): Vital Interests, i.e. If it is necessary to protect someone's life, including that of a third party.	Unlikely to be available to AFBI staff in normal circumstances, this covers, for example, processing in humanitarian emergencies and natural or man-made disasters.
Article 6(1)(e): Necessary to carry out a public task, i.e. to carry out AFBI's official functions or a task in the public interest	<p>Where the processing is necessary to enable AFBI to carry out its core functions, as established in the Agriculture Order 2004. For example, carrying out statutory testing for DAERA.</p> <p>This is likely to be the most commonly-used lawful basis for the processing of personal data by AFBI staff (other than HR staff.)</p>

Lawful basis in GDPR	Illustrations or examples of potential use in AFBI processing
Article 6(1)(f) Necessary for the purposes of the legitimate interests pursued by AFBI, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual”	<p>Available to public authorities such as AFBI only in rare circumstances, although processing the data of a third person in the interests of preventing suspected fraud might be an example.</p> <p>See guidance on the use of this lawful basis at http://afbi.intranet.nigov.net/publications/legitimate-interests-assessment-staff-guidance</p>

In addition, 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, so that processing must be either:

- Article 9(2)(a): with the explicit consent of the data subject;
- Article 9(2)(b): necessary to comply with the data controller’s legal duty in connection with employment;
- Article 9(2)(c): to protect the vital interests of the data subject or another person;
- Article 9(2)(d): carried out by certain non-profit bodies;
- Article 9(2)(e): where the information has been made public by the data subject;
- Article 9(2)(f): in legal proceedings, to obtain legal advice, or exercise legal rights;
- Article 9(2)(g): necessary for reasons of substantial public interest, including carrying out public functions;
- Article 9(2)(h): for medical purposes, including the assessment of the working capacity of an employee;
- Article 9(2)(i): for reasons of public interest in the area of public health; or
- Article 9(2)(j): for archiving in the public interest or for scientific or historical research or statistical purposes.

For more information on choosing a lawful basis, AFBI staff should consult: [Guidance – Consent & other Lawful bases for processing personal data](#)⁸.

More information is available from the [Information Commissioner’s Office](#)⁹.

⁸ Readers without access to the AFBI intranet should contact the Information Governance Unit at info.gov@afbini.gov.uk

⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

APPENDIX 3: AFBI privacy notice template

Data Controller Name: AFBI Address: 18a Newforge Lane Email: info@afbini.gov.uk	Data Protection Officer Name: Glenn Montgomery Telephone: 028 9025 5494 Email: info.gov@afbini.gov.uk
---	--

Why are you processing my personal information?

State the purpose of processing i.e. for disease surveillance or animal welfare purposes

Outline the lawful basis for processing i.e. legislation, contract, public task, vital interests (refer to guidance)

- **ONLY if you are relying on consent to process personal data...**
 - Refer to AFBI Guidance "[Relying on Consent as a lawful basis for processing](#)"
 - Describe how you obtain and record consent.
 - State that they may withdraw consent for this processing, by contacting/by deleting etc...
 - If you do any direct marketing, you need to refer to this in the privacy notice. See [ICO guidance](#).

What categories of personal data are you processing?

List any categories of personal data you are processing e.g. Name, postal address, email address, telephone number, herd number, IP address etc.

What special categories of personal data are you processing?

List any special categories i.e. race/ethnicity, health, trade union membership, genetic data, biometric data, political views, religious beliefs (see [link](#))

Where do you get my personal data from?

State the source of the personal data originates from, and whether it came from public accessible sources.

Do you share my personal data with anyone else?

List the types/names of organisations (internal and external) that you share with and state the reasons for sharing e.g. We may share your data with enforcement agencies for the prevention or detection of crime; We share with DAERA for the purpose of disease surveillance etc.

Do you transfer my personal data to other countries?

Sometimes it may be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the GDPR.

How long do you keep my personal data?

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*).

If personal data is to be held long-term, reference the Data Protection Act 2018 derogations for data processed for scientific research and statistical purposes and explain the measures that will be in place to safeguard the personal information.

How do you use my personal data to make decisions about me?

If you use automated decision making or profiling...

- State any automated decision making or profiling you do
- Outline how decisions are made
- List any consequences

What rights do I have?

Access (Article 15, GDPR)

You have the right to obtain confirmation that your data is being processed, and request access to your personal data by contacting foi.officer@afbini.gov.uk (refer to <https://www.afbini.gov.uk/access-information>);

Rectification (Article 16, GDPR)

You are entitled to have personal data rectified if you believe what we hold is inaccurate or incomplete - please contact us on info.gov@afbini.gov.uk;

Erasure ('right to be forgotten') (Article 17, GDPR)

If you provided your personal data to us either under a contract or with your consent, you have a right to request to have your personal data erased and to prevent processing where your data is no longer required to fulfil the purpose for which it was collected, or where you have withdrawn your consent. Please be aware however, that under GDPR, we are able to continue to process your data if the erasure of such would render impossible or seriously impair the achievement of the objectives of the purposes for which it was collected (i.e. delivering of our public task or scientific research or statistical analysis).

Restriction (Article 18, GDPR)

You have the right to restrict or suppress our processing of your personal data, if you consider the data to be inaccurate or being processed unlawfully by us.

Data Portability (Article 20, GDPR)

Where you have provided your personal data to us either under a contract or with your consent, or we process your data using automated means, you have the right to receive the data from us in a structured, commonly used and machine-readable format, and we will transfer this to another organisation at your request;

Objection (Article 21, GDPR)

You have the right to object to the processing of your personal data if we use it for the purposes of delivering our public task or legitimate interests; however, we retain the right to continue to process the data for scientific research or statistical purposes if this is being carried out for reasons of public interest.

Automated decision-making/profiling (Article 22, GDPR)

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on you, unless you have provided your personal data under a contract or with your explicit consent.

We have published a guide to Citizen's Rights under GDPR/Data Protection Act 2018 which you can access here to get further information:

<https://www.afbini.gov.uk/publications/afbi-guide-citizens-rights-under-gdprdata-protection-act-2018>

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

Or email 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

Web <https://ico.org.uk/global/contact-us/>

APPENDIX 4: 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.
Information Commissioner	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.
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.
Processing	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 2018 and 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	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.