DATA PROTECTION AND INFORMATION SECURITY STAFF GUIDELINES

Title	Data Protection and Information Security Staff Guidelines
Who should use this	All Staff
Author	SAC/Adapted by AVJB
Approved by Management Team	22 August 2018
Approved by Joint Board	N/A
Reviewer	**Assessor & ERO**
Review Date	**2022**

Review History

REVIEW NO.	DETAILS	RELEASE DATE
1		2012
2	CONTROL SHEET ADDED/REVIEWED	OCTOBER 2017
3	UPDATED TO REFLECT NEW ACT AND GDPR. INCLUSION OF INFORMATION SECURITY ADVICE	JULY 2018
4.	REVIEWED NO CHANGE	JANUARY 2020

Introduction

Under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA), the Board and its employees are obliged to adhere to certain principles in order to safeguard the personal data they process.

Personal Data

Personal data includes someone's name, national insurance number, date of birth, health information, criminal records, political views, religion, ethnicity, sexual orientation and trade union membership, for example information provided by members of the public in job application forms, applications to vote and staff HR records.

Processing Personal Information

Processing is an all-encompassing term: it means collecting, storing, sharing, managing, and disposing of personal data (basically doing anything with it).

Data Protection Principles

When handling/processing personal data, Board employees must ensure that they manage personal data in accordance with the following six data protection principles, detailed below. Personal data must be:

- ✓ Processed fairly, lawfully and in a transparent manner
- ✓ Collected for specified, explicit and legitimate purposes
- ✓ Adequate, relevant and limited to what is necessary
- ✓ Accurate and where necessary kept up to date
- ✓ Kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which the data was collected
- ✓ Processed in a manner that ensures appropriate security of the personal data

Data Subjects

Data subjects (e.g. our service users, staff etc) have the right to be informed about the collection and use of their personal data. This is communicated to them in the form of a privacy notice.

Depending on our requirements to collect personal data from our service users/data subjects, they may have the right to ask the Board to:

- Erase their personal information
- Enable the right of data portability
- Correct personal information if it is inaccurate
- Complete personal information if it is incomplete
- Restrict processing of personal information in certain circumstances

Data Subjects also have the right to object to the processing of their personal information.

They may also be entitled to compensation if they suffer material or non-material damage as a result of the Board not adhering to the data protection principles or failing to comply with data subjects' rights.

Subject Access Requests

A data subject can ask for a copy of the personal data we hold about them, along with details of how we gathered the information and who we disclosed it to. This is called a Subject Access Request. We cannot normally charge a fee for this, and have one calendar month to respond. All Subject Access Requests should be forwarded immediately to your Line Manager.

If your job involves you using personal data then your manager will ensure you are given specific training on how to process such data. You must never process personal data beyond the instructions provided by your manager, as this could lead to the Board being fined for breaching the law.

What Are The Board's Responsibilities

All Board staff have a responsibility for protecting personal data including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority.

It is an offence for you to knowingly or recklessly, without the consent of the Data Controller:

- Obtain or disclose personal data or the information contained in personal data, or
- Procure the disclosure to another person of the information contained in personal data.

Board employees are only permitted to access personal data for the Board's business purposes - access for any other reasons may be an offence under Data Protection Law.

The Board is required to report any notifiable breaches of personal data to the Information Commissioners Office (UK regulator of Data Protection law) and has a duty to report any alleged criminal behaviour to Police Scotland.

What Are My Responsibilities

Your Line Manager will tell you what you are allowed to do with the personal details held by the Board and you should follow all instructions carefully. There are strict limits on what information can be stored, used and disclosed and you must not undertake any work on such information without proper authorisation. If you are unsure about any work you are asked to do contact your Line Manager. You should also note that any individual who deliberately breaches the Data Protection Act could be personally responsible for any resulting criminal offence.

The disclosure of personal information will depend on a number of factors and you will be given instructions on what information you can disclose and to whom. If you are not sure if the information can be disclosed you should contact your Line Manager for guidance.

The only exception to the above information disclosure rules is where the information is required urgently to prevent an injury. If you are sure the disclosure will stop an injury from happening you may immediately disclose the personal information. All such emergency disclosures should be reported to your line manager, who will immediately notify the Assessor & ERO and the Head of Valuation Services & Assistant ERO.

The Board's Policies and Procedures in relation to Data Protection and Information Security are available on our Intranet Site. You will also receive training and further guidance on handling personal information in due course.

Sharing Personal Data

Where we agree to share personal data with another Data Controller we MUST have a data-sharing agreement in place. This sets out the responsibilities of all parties.

If we intend to share information with one of the Ayrshire Council's or another Board, for example, we should ensure that we still comply with the Data Protection Principles.

Sometimes we may use a contractor to undertake work on our behalf, which involves personal data being given to the contractor. We remain the Data Controller and the contractor is a Data Processor who undertakes the processing we need them to do. This requires a contract to be in place.

Data Protection Breaches

If there is a breach of the data protection principles the Board could be heavily fined. If staff engage in any activities not sanctioned by the Board those individual staff may be prosecuted or disciplined by not following Board policy.

In the event of a Data Breach you must immediately notify your Line Manager who will immediately notify the Assessor & ERO and the Head of Valuation Services & Assistant ERO.

Most breaches occur by accident, either by the organisation not having proper systems in place or as a result of human error. In the event of a data breach the Board's Data Protection Officer – Service Lead (Democratic Governance) - must be informed.

Information Security

In order to keep personal data safe and secure, sensitive personal records should be stored in locked filing cabinets with restricted access. Where personal data has been taken off-site, this will be restricted to only what is necessary to undertake the required task.

Transportation of Personal Information

- ✓ Should you be responsible for the transportation of confidential/sensitive information then you must take precautions to protect the information at all times.
- ✓ No sensitive files or information should be left in an employee's car unattended. To minimise risk of loss you should only take the information that you require.
- ✓ Should it be necessary to hold on to files/ information overnight then the files/ information must to taken to the employee's home and stored in a safe place, where family members or others etc. cannot access them. Information must not be left unattended in their car overnight.
- ✓ The data must be kept secure at all times. Electronic records should be held only on encrypted USB drives, approved for use by the Board, or electronic devices such as secure Board laptops. This electronic information should not be accessed while in public (e.g. when on public transport where others could view the information on the screen).
- ✓ If you are disposing of paper copies stop and think if these contain personal data or confidential information, if so, you must dispose of this information by using the confidential waste bins provided for shredding to ensure that information is disposed of in compliance with data protection legislation.

Upon your commencement of employment with Ayrshire Valuation Joint Board, you will have access to the Board's Policies and Procedures in relation to Data Protection and Information Security. These provide all employees with further guidance and information on security measures for handing personal data such as emailing, posting, removing information from the office, copying and destroying personal data and are available on the Board's Intranet site - SharePoint.

Data Protection/Freedom of Information/Records Management

You should be aware that Data Protection, Freedom of Information and Records Management Laws are quite separate but are closely linked.

As indicated above, the use of personal and commercially sensitive information is strictly defined and controlled under the terms of the Data Protection legislation. Whilst the Board continually strives to remain open and transparent in an effort to meet its obligations under Freedom of Information Legislation, it nevertheless recognised that it has equally important obligations under the terms of Data Protection Legislation.

You should be aware that the Board has very serious responsibilities and obligations under Freedom of Information, Data Protection and Records Management Legislation, therefore, you should always refer any requests for information made under the Freedom of Information Acts or the Data Protection Acts to your Line Manager who in turn will refer the matter to the Assessor & ERO and the Head of Valuation Services & Assistant ERO.

Finally

You will receive additional training on Data Protection, Freedom of Information and Records Management in due course. Remember also that there are lots of helpful information on these important issues on the Board's Intranet Site.

Remember, if you are in any way not sure – ask for help.