ELLESMERE TOWN COUNCIL

Miss Joanne Butterworth
Town Clerk & RFO
1-3 Willow Street
Ellesmere
Shropshire
SY12 0AL

Tel: 01691 622689
Email:jo.butterworth@ellesmere-tc.gov.uk

Data Protection Policy

A) INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR), 25th May, 2018.

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- Personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject (ie a living individual)
- All personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes
- The personal data collected and retained must be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed
- All personal data collected must be accurate and, where necessary, kept up to date
- The personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data are processed
- Personal data must be processed in a manner that ensure 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

D) TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:
i) job title and job descriptions
ii) your salary
iii)your wider terms and conditions of employment
iv)details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
v) internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from the Town Clerk. The Town Council's Retention Policy was updated on the 4th June, 2018 to reflect the new General Data Protection Regulations on the 25th May, 2018.

E) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:
a) the right to be informed about the data we hold on you and what we do with it;

b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data. More information can be found on each of these rights in our separate policy on employee rights under GDPR.

F) RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection. We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

G) LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity. Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data. However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

H) ACCESS TO DATA - SUBJECT TO ACCESS – DATA SUBJECT RIGHTS

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Subject Access Rights

To comply with the new GDPR rules the council will need to update procedures to ensure they cover the handling of subject access requests and ensure the following:

- In the majority of cases the council will not be able to charge a fee for complying with a SAR, which is a right of access to the individual's personal data held by the council as data controller
- The council will have 1 month to comply with a SAR (up to May 25th, 2018 the deadline is 40 days)

- The council can charge a fee for requests that are manifestly unfounded or excessive or repetitive and can refuse to respond
- If the council refuses a request, the individual must be told why and informed of their right to complain to the ICO and to a judicial remedy. The individual must be informed of the decision without undue delay and at the latest within 1 month. Data Subject Rights In addition to being able to submit SARs described above data subjects have the rights to:
- restrict processing of their personal data - new limited rights against data processors
- object to processing of their personal data for direct marketing purposes
- not be subject to automated decision-making
- receive compensation form the data controller AND the data processor for the damage suffered as a result of an infringement of the GDPR
- obtain from a data controller without undue delay the rectification of inaccurate personal data
- ask the data controller to erase their personal data and to no longer process it (the right to be forgotten). This could be where the data is no longer necessary in relation to the purpose for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the GDPR. However, further retention of the personal data will be lawful in certain circumstances. For councils, an example is where the data is required for compliance with a legal obligation. Where the data controller has made the personal data public and is obliged to erase the personal data it shall take reasonable steps to inform data controllers and processors who are processing the personal data that the data subject has requested them to erase any links to, or copy or replication of that personal data
- be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights
- data portability ie to receive a copy of personal data or to transfer personal data to another data controller

I) DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:
i) any employee benefits operated by third parties;
j) disabled individuals - whether any reasonable adjustments are required to assist them at work;
k) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
l) for Statutory Sick Pay purposes;
m)HR management and administration - to consider how an individual's health affects his or her ability to do their job;
n) the smooth operation of any employee insurance policies or pension plans;
o) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

J) DATA SECURITY - BREACHES

All our employees are aware that hard copy personal information is kept in a locked filing cabinet, drawer, or safe. Employees are aware of their roles and responsibilities when their role

involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people. Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received.

Where personal data is recorded on any such device it should be protected by:
a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Data Breaches

The council as data controller will notify the ICO where a data breach is likely to result in a risk to the rights and freedoms of the individuals affected. Therefore, the council as a data controller should detect, report and investigate a personal data breach. Data controllers will be required to report to the ICO without delay and definitely within 72 hours, any identified personal data breaches. In some cases data breaches will need to be reported to the data subjects where the breach is likely to result in a high risk to the rights and freedoms of individuals.

A data processor must also notify a data controller without undue delay after becoming aware of a personal data breach. The data breach must be investigated, and procedures put in place to ensure such a breach does not recur.

Failure to report a breach when required to do so could result in a fine, as well as a fine for the data breach, then it would be better for the council to err on the side of caution when deciding on whether to report data breaches to the ICO, and certainly to consult the ICO on whether the breach needs to be reported.

The Town Council and their Data Protection Office have compiled a data inventory to evidence compliance with the GDPR and new rights of the data subjects.

K) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

L) INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

M) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach. More information on breach notification is available in our Breach Notification policy.

N) TRAINING

New employees must read and understand the policies on data protection as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR. All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

O) RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

P) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:
JDH Business Services Ltd
Carreg Lwyd
Cefn Bychan Road
Pontymwyn
Flintshire CH7 5EW

Q) Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Ellesmere Town Council exceeds this turnover but will never the less ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities

- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

Adopted by Council: Ellesmere Town Council on: Monday 4th June, 2018

Review Date: May, 2019