Ringwood Town Council

# *Data Breach Procedure*

Adopted on: 17th April 2019

---

## 1. Introduction

If personal data held by the Council is mishandled, the law requires that it respond in certain ways. This document sets out how the Council will meet its legal obligations should such a situation ever arise.

## 2. What is a data breach?

The mishandling of personal data ("a data breach") can happen in many ways. The following list describes some of the most common (it is not a complete list):

- Sending or copying an email to an unintended recipient;
- Copying an email to recipients using "cc" rather than "bcc";
- Accidental loss or theft of a memory stick, laptop computer, CD-ROM, etc.;
- Unauthorised persons gaining access to physical or electronic records (e.g. in the course of a burglary or computer hack);
- Accessing records for no proper purpose (e.g. staff may need to consult records for a legitimate purpose but it may be illegal for them to do so out of idle curiosity);
- Improper deletion or alteration of records (including by malicious persons or software);
- Ignoring or mishandling a legitimate request for data to be corrected or deleted.

Sometimes it is obvious when a data breach has happened but this is not always the case. In case of doubt (that is, if you think that a data breach **may** have happened but are not necessarily sure) then you must follow this procedure.

## 3. Who does this procedure apply to?

If you work for the Council (whether as an employee, a worker or a free-lancer or contractor) then this procedure applies to you. Failure to do so without a lawful excuse may result in disciplinary or enforcement action being taken against you. In a sufficiently serious case this could result in dismissal without notice or immediate termination of your contract for services.

Councillors are also required to conduct themselves in accordance with this procedure. Failure to do so without a lawful excuse or impeding staff in the application of the procedure may amount to a breach of the Code of Conduct.

## 4. What to do if a data breach is known or suspected

If you have reason to believe that a data breach has happened or may have happened you **MUST** complete a Data Breach Report Form (see form below).

**DON'T** worry if you cannot fill in every part of the form fully – fill in as much as you can.

**DON'T** delay – this is more important and urgent than anything else you may have to do (apart from medical emergencies or immediate threats to someone's physical safety)

**DO** send the completed form to the Town Clerk and the Deputy Town Clerk as soon as you can - if possible by email to:

chris.wilkins@ringwood.gov.uk and

jo.hurd@ringwood.gov.uk

If this is not possible, deliver hard copies to them in person (or leave them on their respective desks if they are not immediately available).

## 5. Responding to a Data Breach Report

Upon receiving a Data Breach Report Form the Town Clerk and the Deputy Town Clerk will speak to each other and agree which of them will take responsibility for the subsequent handling of the matter (where this is not possible responsibility will fall on the Town Clerk unless he or she is unavailable for any reason in which case responsibility shall devolve to the Deputy Town Clerk). The responsible officer will then invoke and follow the Data Breach Checklist & Action Plan set out below.

# Ringwood Town Council – Data Breach Report Form

| | |
|---|---|
| Details of breach<br><br>(Describe briefly what has happened or how the data breach arose with dates and times where possible) | |
| Nature and content of data involved<br><br>(Describe the type(s) of personal information involved e.g. email addresses, payroll information, medical information, etc.) | |
| Number of individuals affected | |
| Name of person making this report | |
| How and to whom this report was submitted | |
| Date and time this report was submitted | |

# Ringwood Town Council – Data Breach Checklist & Action Plan

| | |
|---|---|
| Date and time of Notification of Breach | |
| Notification of Breach received from<br><br>Name<br><br>Contact Details | |
| Report form attached? | |
| How and when report acknowledged | |
| Name of person investigating breach<br><br>Name<br>Job Title<br>Contact details<br>Email<br>Phone number<br>Address | |
| Further information about breach (not contained in report form) | |
| Information Commissioner informed, if relevant<br><br>Time and method of contact<br><br>https://report.ico.org.uk/security-breach/ | |

| | |
|---|---|
| Police Informed if relevant<br><br>Time and method of contact<br><br>Name of person contacted<br><br>Contact details | |
| Individuals contacted<br><br>How many individuals contacted?<br><br>Method of contact used to contact?<br><br>Does the breach affect individuals in other EU member states?<br><br>What are the potential consequences and adverse effects on those individuals?<br><br>Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved. | |
| Staff briefed | |
| Assessment of ongoing risk | |

| | |
|---|---|
| Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data | |
| Recovery Plan | |
| Evaluation and response | |