Birchanger Parish Council
Subject Access Request Policy

Version 1.0
6tn November 2018

Document History

Version	Date	Remarks
1.0d1	6th November 2018	Candidate for adoption

Next review date: November 2020

Introduction

This policy describes the process to be followed when a subject access request (SAR) as defined by the General Data Protection Regulations (GDPR) is received by the council.

What is a subject access request?

A subject access request is a formal request by an individual that we send them a copy of the personal data that we hold about them. Personal data is defined here as it is elsewhere in GDPR and can be considered as any data, in whatever form (computer or other 'filing system') that belongs to an identifiable living person. Examples include names, contact details and financial information.

How are we notified of a subject access request?

A person making an SAR should contact the clerk of the council requesting a copy of any data we hold about them. The clerk should treat anything that looks like an SAR request as if it was a formal request; in other words we should not try to get out of complying just because the right words weren't used, or because of the way they contacted us.

Meeting the SAR

Upon receiving an SAR the clerk must first take any necessary steps to ensure that the person making the request really is the subject, and not an imposter. Once satisfied the clerk will conduct a search for the information requested. The extent of the search will depend on the request; if only data relating to a certain topic, event or time period is requested then the search will be limited. If all data about the person is requested than all sources of data will need to be searched. This includes

- Copies of the electoral roll
- The web site[1]
- Emails about or mentioning the person held by clerk and council. This includes personal email accounts if the emails in question were conducting council business.

The clerk may need to request the help of councillors in compiling the data.

Once the search is complete the clerk will send the requested data to the requestor by the most appropriate means. Normally a request by email will receive a reply by email containing copies of the requested data and scans of physical documents; requests by letter will receive a printed reply.

The reply will inform the requestor that we believe that we have complied with their request to the best of our knowledge but that they may complain to us and ultimately the ICO if they feel we have not.

Timescales

The clerk should meet the request as soon as possible and always within 30 days. If the response looks as if it will take some time (i.e. over 14 days) then the clerk will contact the requestor and inform them that that is the case.

[1] The site currently holds no personal data, but that may change

Fees

No fees may be charged unless the person concerned is making repeated or otherwise vexatious requests. In this case then the clerk will confer with the council to agree:

1. Whether the request really is repeated or vexatious
2. What would be an appropriate fee, which may only take into account actual time and costs incurred

Records

A record of all SARs received and their responses will be maintained by the clerk to the council.

Breach Handling Process

The breach handling process is as follows.

The very first thing to do is to decide whether the allegation is credible. If the person reporting the breach is a committee member then there will be an assumption that the report is genuine. If the report comes from elsewhere a very rapid (same working day) assessment must be undertaken to eliminate obviously spurious or ill-founded notifications. If the notification fails this initial assessment then the person who notified us will be told of the outcome of our investigations.

In any case the trustees must be informed that a suspicion of a breach has occurred, and they should be told the nature of the breach.

Assuming that the breach notification has not been rejected, the first priority is rectification and damage limitation. If the cause of the breach is obvious and can be resolved, then this step is easy. If ongoing and/or not easy to solve, for example somebody gaining access to our website via an unknown route, then it may be necessary to take the service down until the source of the problem has been identified and corrected.

At a very early stage an assessment must be made of:

- Whose personal data has been compromised?
- How damaging could this breach be to them?

The chairman must make this determination. He will probably do so by discussing the matter with other trustees and may seek outside professional guidance if necessary. Based on all of the facts a decision will be made as to whether the matter must be reported to the ICO. This is a decision that may have serious consequences, so the chairman should read the latest IPO guidance, and should ensure that trustees are fully involved.

If it is decided that the breach must be reported to the Information Commissioner then the report must be made within 72 hours of the initial report of the breach. No allowances are made for holidays or weekends.

Informing the Members Concerned

Any member whose personal data has been affected by a breach should be notified. The notification should tell them what has happened, how it could adversely affect them and what we are doing to remedy the situation. They should also be informed that they have the right to complain to the Information Commissioner's Office.

Record Keeping

A file of all decisions, with reasoning, should be kept of each breach or suspicion of a breach by the chairman.