MACCLESFIELD TOWN COUNCIL

SUBJECT ACCESS REQUEST POLICY

DOCUMENT VERSION CONTROL

Document Title: Subject Access Request Policy

Version No.	Date Change Made	New Version No.	Changes Made By (initial)	Comment
00.01	May 2018		HW	New policy for GDPR

CONTENTS

Contents

1. Introduction

1.1 Under the General Data Protection Regulation (GDPR), individuals have the right to know what data controllers hold on them, why their data is being processed and whether it will be or has been given to any third party. They have the right to be given this information in a permanent form (hard copy).

1.2 This is known as a 'subject access request' or "SAR".

1.3 The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63 – see annex).

2. Responsibilities

2.1 Councillors and officers must be aware of and follow this policy.

2.2 Personal data or Personally Identifiable Information (PII) controlled by Macclesfield Town Council will be easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

2.3 Standards and templates will be implemented to ensure timely responses to SARs.

2.4 Data subjects are informed of their right to access data – this is documented in Macclesfield Town Council's Privacy Notice.

3. Subject Access Requests (SARs)

3.1 A SAR must be in writing; either by email, letter or even social media. The request does not have to expressly state it is a "subject access request" but must be dealt with as such.

3.2 Any verbal request made must be followed up in writing as this a GDPR requirement.

3.3 A data subject will not be asked to complete a form or template – their written request is sufficient.

3.4 If a disabled person is unable to fulfil the requirement for a written request, a verbal request will be accepted.

3.5 If a SAR comes from a minor (currently under the age of 16 but may change to 13 under UK derogation), the PII still belongs to the child. If it is considered that the child is mature enough, the response will be sent to them and not parent or guardian.

3.6 All councillors and officers must be able to recognise a SAR and immediately inform the Clerk of the request. No one officer will be tasked with responding to a SAR although a single officer will be tasked with coordinating the response.

3.7 A SAR can be followed by a request to stop processing or erase the data subject's PII.

4. Response time

4.1 A SAR response must be given in one month from the point at which all the information has been provided (including proof of ID) to enable the search.

4.2 A further two months may be added if Macclesfield Town Council can demonstrate exceptional circumstances, but the data subject must be notified of this within the first month and an explanation of why extension is necessary, how long this is expected to take and what they can do if they are dissatisfied.

5. SAR Response

5.1 As a minimum the SAR response must include:

- The PII data held,
- The purpose of why it is held/collected,
- Who else has their PII,
- The retention policy,
- The subject's rights,
- The contact details of the DPO.

6. Fees

6.1 A fee will not be charged unless it can be demonstrated that the SAR is unfounded, or made multiple times or excessively.

6.2 A fee may be charged if multiple copies are required for the same information.

7. Proof of identity

7.1 Proof of identity is required following a SAR. The request for proof of ID will be reasonable and ideally be photo ID.

7.2 If the data subject is well known to Macclesfield Town Council (e.g. a long standing volunteer) then ID may not be required.

8. Refusing a SAR

8.1 A SAR can be rejected if it would adversely affect the rights of others e.g. intellectual property or trade secrets, or it is unfounded or excessive.

8.2 If Macclesfield Town Council can demonstrate grounds for refusing to action a SAR request, the data subject must be informed within 1-3 months with an explanation of why the request was refused.

9. Exemptions

9.1 Data may be restricted for the following categories of data when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard. (This may be further clarified by the ICO or derogation by UK Law.)

- National security
- Defence

- Public security
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security
- Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or Member State, including monetary, budgetary and taxation matters, public health and social security,
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions,
- A monitoring, inspection or regulatory function connected to the exercise of official authority in the case of national security, objectives of general public interest of the Union or of a Member State or monitoring of regulated professions,
- The protection of the data subject or the rights and freedoms of others,
- The enforcement of civil law claims.

10. Third party data

10.1 Care must be taken to protect the rights of third parties when responding to a SAR.

10.2 Either gain third party's permission or erase their PII.

10.3 Answer these questions before responding to a SAR:

1. To satisfy the request, will there be a need to disclose a third party?
2. Has the third party given consent?
3. After careful consideration, is it reasonable to respond without the consent of the third party?

10.4 All decisions must be documented.

11. Council employees

11.1 Macclesfield Town Council employees may also make a SAR e.g. about confidential data held about them.

12. Overview of the SAR response

12.1 The following is an overview of the steps that will be followed on receipt of a SAR.

1. **Forward** the SAR immediately to the Clerk,
2. **Request** proof of ID,
3. If required, **clarify** the request,
4. Make a full exhaustive **search** of all records,
5. All the personal data that has been requested must be **provided** unless there are grounds for refusal or an exemption can be applied,
6. ***Respond*** within one calendar month after accepting the request as valid,
7. Subject Access Requests will be undertaken **free of charge** to the requestor,
8. If requested by the data subject, **stop** processing or **erase** their data,
9. Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

13. SAR database

13.1 All requests will be logged on a SAR database.

13.2 The database will be maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.

13.3 The database will also record the form of ID checked for proof of identity.

14. Types of ID

14.1 Macclesfield Town Council accepts the following forms of identification.

(* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence / Shotgun Certificate
- EEA National Identity Card
- Full UK Paper Driving Licence
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*
- State/Local Authority Educational Grant Document*
- HMRC Tax Notification Document
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company+
- Judiciary Document such as a Notice of Hearing, Summons or Court Order
- Utility bill for supply of gas, electric, water or telephone landline+
- Most recent Mortgage Statement
- Most recent council Tax Bill/Demand or Statement
- Tenancy Agreement
- Building Society Passbook which shows a transaction in the last 3 months and your address

15. Searching records

15.1 Electronic records

PII held in	ICO guidance
Archived/backup records	Should be included in SAR response
BYODs	Currently no expectation to search personal emails or personal devices as part of the response. ICO advise that PII is not processed on BYOD
Emails	Must form part of the SAR response, including searching the deleted folder
Files	Must form part of the SAR response
Deleted records	Records that have been deleted are not accessible by the organisation without specialist technologies

15.2 Non-electric records

PII held in	ICO guidance
Filing systems	Should be searched if there is a system in place that allows the organisation to find information, applying a standard search procedure, without searching through every item in a set of information. As long as specific information within the set is readily accessible the set of information will be data in a relevant filing system even if the information needs to be obtained from several different locations within the system.

16. Procedure for handling a SAR

16.1 Upon receipt of a SAR Macclesfield Town Council will:

1. Verify if we are the controller of the data subject's personal data. If not, we will inform the data subject and refer them to the actual controller.
2. Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
3. Verity the access request; is it sufficiently substantiated? Is it clear to the what personal data is requested? If not: request additional information.
4. Verify whether requests are unfounded or excessive. If so, we may refuse to act on the request or charge an administrative fee of £25.
5. Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
6. Verify whether we process the data requested. If we do not process any data, inform the data subject accordingly.
7. Ensure data will not be changed as a result of the SAR. (Routine changes as part of the processing activities concerned are permitted).
8. Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject. If data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

17. Responding to a SAR

17.1 The response must be in writing and delivered securely – either by encrypted email or by recorded delivery, addressed to the data subject.

17.2 Respond to a SAR within one month after receipt of the request:

1. Depending on the degree to which personal data is organised and structured, we will search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc.

2. Personal data will not be withheld because it is believed it will be misunderstood; instead, we will provide an explanation with the personal data. We will provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data will be supplied in a permanent form except where the data subject agrees or where it is impossible or would involve undue effort. We may ask the requester if they can view the personal data on screen or inspect files on our premises. We will redact any exempt personal data from the released documents and explain why that personal data is being withheld.

3. If more time is needed to respond to complex requests, an extension of another two months is permissible, we will communicate this to the data subject in a timely manner within the first month.

4. If we cannot provide the information requested, we will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

5. If data on the data subject is processed, the following will be included as a minimum in the response:

   i. the purposes of the processing;

   ii. the categories of personal data concerned;

   iii. the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses;

   iv. where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

   v. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

   vi. the right to lodge a complaint with the Information Commissioners Office ("ICO");

   vii. if the data has not been collected from the data subject: the source of such data;

   viii. the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

18. Complaints

18.1 When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office (ICO) if they remain unhappy with the outcome.

19. SAR Quick Reference

Action	GDPR regulation
Fee	No fee
Response time	One month
Extensions to response time	Extension of a further two months permitted for complex requests. Must inform the data subject within the first month and the reason for the delay
Unfounded or excessive requests	Can charge a reasonable fee or refuse to act on the request
Declining a request	Must inform the data subject within one month with the reason for the refusal
Identity of data subject	If in doubt, request proof of ID
Form of response	Must be concise, transparent, intelligible and easily accessible, using clear and plain language, particularly if addressed to a child
Format of response	In writing, either by encrypted email or recorded delivery

20. Annex: Recital 63

20.1 A data subject should have the right of access to personal data which has been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

20.2 This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.

20.3 Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

20.4 Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.

20.5 That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.

20.6 However, the result of those considerations should not be a refusal to provide all information to the data subject.

20/.7 Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.