Marlborough Town Council

16 January 2024

Dear Councillor

Full Town Council

I hereby **summon** you to a meeting of **Marlborough Town Council** which will be held on **Monday, 22 January 2024 at 7pm** in the **Court Room** Marlborough Town Hall.

Yours sincerely

Richard Spencer-Williams

Richard Spencer-Williams, PSLCC

Town Clerk

If members of the public wish to attend they should notify the Town Clerk of this by noon on the Friday prior to the meeting. Some members of the public may not be allowed to attend if all the allocated seats are taken.

If members of the public wish to attend and ask a question they should also notify the Town Clerk prior to the meeting and provide their question in writing at the same time. If members of the public wish to ask a question but not attend, they can provide the question in writing to the Town Clerk by noon on the day of the meeting and a written response will be provided.

PRAYERS

PUBLIC QUESTION TIME

In accordance with Standing Order 3(f), members of the public may ask questions of the Council. The time allocated for this should not exceed 10 minutes and be limited to 1 question per person unless directed otherwise by the Chair. A full response may not be possible without further research, and the Chair may direct that a written or oral response be given.

CRIME AND DISORDER

A member of Wiltshire Police will be invited to give a report and answer questions from Councillors and members of the public (not to exceed 10 minutes)

PRESENTATION FORESTRY ENGLAND

A Presentation by Nicky Morgans from Forestry England on their Management Plans for Savernake Forest followed by Q&As from Councillors

TO RECEIVE QUESTIONS TO AND FROM WILTSHIRE COUNCILLORS

Not to exceed 10 minutes

AGENDA

1. **Apologies for absence**

2. **Declarations of interest**

   a) To receive any Declaration(s) of Interest under Marlborough Town Council's Code of Conduct issued in accordance with the Localism Act 2011

   b) To consider any dispensation requests received by the Town Clerk
   Members are reminded that they are obliged to notify the Monitoring Officer of a change to disclosable interests, or a new interest as defined in Appendices A and B of the Code of Conduct within 28 days of becoming aware of it. These should be passed on to the Town Clerk to register online.

3. **Mayor's Announcements**

4. **Minutes**

   To approve and sign the minutes of the meeting held 8 January 2024

5. **Action Log**

   To note and review the Action Log

6. **Town Mayor 2024-25**

   To select the Town Mayor for the forthcoming municipal year 2024/25

7. **Grants Policy**

   To consider the updated Grants Policy for adoption

8. Information Management Policies

To consider information management policies for adoption

9. Community & Youth Centre

To consider the proposal by Wiltshire Council to asset transfer the Community & Youth Centre to Marlborough Town Council

10. Outside Bodies

An opportunity for Councillors to give reports on recent interactions

11. Committee Minutes

In accordance with para 3.1 of the Scheme of Delegation, to note the approved minutes of the following committee meetings: **Planning** – 16 October 2023, 13 November 2023, 4 December 2023; **Amenities and Open Spaces** – 9 October 2023. These minutes have been approved by committees and circulated to Members and are available to download from https://www.marlborough-tc.gov.uk/council/meetings-agendas-minutes-from-may-2023 or from the Town Council offices. Other meetings have taken place, but minutes are not yet approved so remain in draft form.

12. Members Question Time

Questions to be submitted to the Town Clerk no later than midday on the day of the meeting. Not to exceed 10 minutes

13. Common Seal

To authorise the fixing of the Common Seal of Marlborough Town Council to all documents necessary to give effect to the decisions of the meeting

To approve and sign the minutes of the meeting held 8 January 2024 (with one proposed amendment):

Marlborough Town Council

Full Town Council

Minutes of an extraordinary meeting of Marlborough Town Council held Monday, 8 January 2024 in the Court Room, Marlborough Town Hall at 7pm

PRESENT	Councillor Nicholas Fogg	Town Mayor
	Councillor Andrew Ross	
	Councillor Noel Barrett-Morton	
	Councillor Lisa Farrell	
	Councillor Mervyn Hall	
	Councillor Kym-Marie Cleasby	Deputy Mayor
	Councillor Jane Davies	
	Councillor Caroline Thomas	
	Councillor Mark Luson	
	Councillor Susannah O'Brien	
	Councillor Emily Trow	
	Councillor Bethany Kohrt	
	Richard Spencer-Williams	Town Clerk
	Dawn Whitehall	Corporate Services Officer
ALSO PRESENT	Neil Goodwin	Marlborough.News
	Plus 6 members of the public	

PRAYERS

The Town Mayor opened the meeting with prayers.

PUBLIC QUESTION TIME

There were no questions.

QUESTIONS TO AND FROM WILTSHIRE COUNCILLORS

Councillor Hall asked whether there would be a full enquiry into what had caused the river surge leading to the flood on 5 January. **Councillor Thomas** believed the

Environment Agency would conduct a review to understand what happened, although given the amount of flooding incidents across the whole country this may take some time.

Councillors Davies and **Thomas** praised the work done in response to the flood on 5 January and thanked Town Council staff. They asked questions including whether there was a flood plan or emergency resilience plan; were there Flood Wardens; whether to review the number of gel sacks or cones and other first-line response equipment (e.g. tabards, walkie-talkies, signs) held by the Town Council. The **Town Clerk** confirmed the flood plan formed part of the emergency plan, and that Wiltshire Council had a copy.

Councillor Cleasby had taken up the role of Flood Warden in a previous term but had had to step back from the role. She had personally set up an online fund seeking donations to support people without flood insurance and asked whether the Town Council could administer it.

Councillor Ross confirmed that a Community Emergency Plan had been covered in the previous council term, and that Scottish & Southern had presented to the Council about services and resources available during emergencies.

The **Town Clerk** was in close liaison with Wiltshire Council officers, and the Town Council staff team had met earlier that day to review the situation and agree further actions, including discussing how to engage the wider community after receiving offers of help from volunteers. Targeted communications would continue. The team had also reached out to replenish its stock of gel sacks.

It was agreed that Councillors should be involved in a review as soon as possible and the **Town Clerk** agreed to circulate relevant information and set up an extraordinary meeting for the following week.

365/23 APOLOGIES

Apologies for absence were received from **Councillors Cooper, Sheppard** and **Shantry**.

366/23 DECLARATIONS

There were no declarations of interest or requests for dispensation.

367/23 MAYOR'S ANNOUNCEMENTS

The **Mayor** thanked staff who had made huge efforts during the flooding on Friday with very little notice – they had gone well beyond the call of duty. With flooding in mind, he questioned whether the site in the emerging local plan near Elcot Lane, allocated for a housing development, should be reconsidered in the light of the risk of building near a river, and the impact of the built environment in contributing to flooding. It was however good news that the requirement to build a set number of houses without referring to local conditions had been revoked.

The Marlburian Club magazine had an interesting article about Herbert Leaf, a former Mayor and great benefactor to the town, having left a bequest that was still active. He

asked whether the photograph used, which showed him in his Mayoral robe with the maces, might be used to replace the current photograph in the Council Chamber.

368/23 MINUTES

RESOLVED: that the minutes of the meeting held 6 November 2023 were confirmed as a true record and signed by the Town Mayor

369/23 BUDGET AND PRECEPT 2024 25

Members noted the Town Clerk's report and thanked all involved in preparing the budget.

Councillor Thomas, Chair of the Finance & Policy Committee, explained the background to the preparation of the budget (including ongoing cost of living crisis; inflation; local government pay increases; staff costs). In addition to maintaining existing services, Councillors were asked to consider new or aspirational projects or areas of service delivery.

Potential additional costs from proposed developments, events and projects were:

- Town Hall 'hidden room' feasibility study - £3,000
- Youth work apprenticeship and provision - £30,000
- Re-enactment event - £20,000

In arriving at the recommended budget to put forward, the Finance & Policy Committee had included the Town Hall study, reduced the youth work by 50% to start mid-year and excluded the re-enactment event for 2024 25 based on uncertainty of likely actual costs, having not had sight of a detailed costed proposal.

[1]The recommended budget for Councillors to consider therefore totals £890,930, representing a 6.54% rise on the current Band D household. This would make the Town Council precept for a Band D property £246.97 per annum, which is an additional £15.27 per household above 23/24.

Members debated the re-enactment event and whether to include it. Comments included:

- The event would bring the town together and celebrate its history
- It aligned with one of the Town Council's priorities - heritage
- It was hoped that financial sponsorship could be obtained
- No decision had been taken not to host the event; the proposal was not to include it in the 2024 25 budget year
- No other town wide events were planned for 2024 25; whether it was important to have an event each year
- Any costed proposal would need approval by Full Council prior to going ahead, but if it wasn't in the budget it couldn't be proposed
- Whether the Heritage Ear Marked Reserve could be used should a costed proposal come forward during the year

[1] Proposed text to replace the draft circulated on 11 January

- That the youth work had also been reduced: youth work would provide benefit all through the year rather than a one-off event

RESOLVED: that Committee Budgets are agreed as proposed, and that a net budget precept requirement to levy to Wiltshire Council for 2024/25 be £890,930

The precept increase is equivalent to 6.54% for a Band D property (£246.97 per annum; an increase of £15.27)

370/23 COMMITTEE MINUTES

In accordance with para 3.1 of the Scheme of Delegation, Members noted the approved minutes of the following committee meetings: **Planning** – 22 August, 4 September and 25 September 2023; **Property** – 23 October 2023 and **Finance and Policy** – 31 October 2023.

371/23 MEMBERS' QUESTION TIME

No questions had been submitted.

372/23 COMMON SEAL

Proposed by **Councillor Ross** and seconded by **Councillor Barrett-Morton** and **RESOLVED:** that the Common Seal of Marlborough Town Council be affixed to all documents necessary to give effect to the decisions of the meeting

The meeting closed at 7.45pm

ITEM 5 ACTION LOG

To note and review the Action Log

Ref	Detail	Min #	Owner	Status	Meeting date	Notes
185	Ask WC for advice on how to progress matter of Marlborough Community & Youth Centre	232/23	Town Clerk	In Progress	25 09 2023	26 9 23 TC emailed WC Assets team. TC meeting relevant officer at County Hall 2 11 23 to clarify respective positions and way forward. Letter sent by RSW on 17 11 23 requesting asset transfer for nominal sum, with outline reasons and legal power specified. **Email reply received from WC Assets Team - on agenda 22 1 24 for resolution**

201	Clarify when/for how long police touchdown point has personnel on site (as opposed to open to the public)	Crime & Disorder	Town Clerk	Complete	06 11 2023	**Emailed Police 7 11 23. Reply received 7 11 23. Opening times confirmed as Mon 9-12am/1-5pm, Wed 9-12.30pm, Fri 9-12pm/1-5pm; with advisory that due to staff shortages there may be disruption to these times.**
202	Circulate Swindon 105.5 DAB info	309/23	Corporate Services Officer	Complete	06 11 2023	**Circulated 7 November 2023 by email**
203	Pass on thanks to all involved in AGAR audit	315/23	Town Clerk	Complete	06 11 2023	**Town Clerk conveyed 7 11 23**

ITEM 6 TOWN MAYOR 2024-25

To select the Town Mayor for the forthcoming municipal year 2024/25

Nomination: Deputy Mayor Cllr Cleasby

The Council are asked to support the proposal by Cllr Farrell, and seconded by Cllr Shantry, and instruct the Town Clerk accordingly.

Town Clerk 12 1 24

ITEM 7 GRANTS POLICY

To consider for adoption the updated Grants Policy

Purpose

The purpose of this report is to consider the proposed amendments to the existing Council Grants Policy, as recommended by the Finance and Policy Committee for adoption.

Current Status/ Considerations

The Finance and Policy Committee reviewed the Grants Policy on the 31 October 2023.

Below is the current policy with proposed amendments highlighted for consideration:

Marlborough Town Council Grants Policy

1. Introduction

1.1 Marlborough Town Council has the power to provide grants under its General Power of Competence *(Localism Act 2011)*. And section 137 of the Local Government Act 1972.

1.2 The Council is committed to supporting local voluntary and community groups working towards improving and enhancing Marlborough in line with the Council's priorities and that have a specific benefit to residents of Marlborough.

1.3 Marlborough Town Council budgets a sum of money every year for grants which are made available to organisations for financial assistance. The Council acknowledges that some organisations, particularly new or smaller ones, may experience difficulty in completing the application requirements and help will be offered with the process.

1.4 Marlborough Town Council will:

- Publicise its grant opportunities widely throughout the town
- Review this policy and application process Every three years

2. Criteria

2.1 Applications must be for defined projects that benefit the local community

2.2 An organisation may only submit one application for a grant in any one Financial Year

2.3 The organisation must be non-profit making

2.4 Grants are not made retrospectively for completed projects

2.5 The organisation must demonstrate a clear need for financial support and typically show how fund raising has taken place.

2.6 Organisations will need to provide evidence of a constitution or terms of reference-and hold a bank account specific to the applying organisation or community group (or be able to demonstrate they are support by an organisation who will 'host' the award funds).

2.7 Organisations applying will need to provide a set of audited accounts for the previous Financial Year and any other financial information as requested by the Town Clerk. Organisations just starting up must submit basic financial information (e.g. a bank statement)The Council may ask for further information or estimates from contractors for work to be undertaken

2.8 All grant funding must be claimed by successful applicants before 31st March and any unused monies not used for the purpose intended should be returned to the Town Council

2.9 Applicants must acknowledge Marlborough Town Council's financial support in any publicity or printed material

2.10 A report must be made about how the grant has been used to the Council within 12 months of the award. Failure to do this may jeopardise future grant applications

2.11 The Town Council will not consider grant applications for:

a) Political or religious activities
b) Statutory bodies to fund core services
c) A private profit making/commercial organisation
d) Existing Running costs - e.g., rent, rates, electricity, etc.
e) Projects that have already been completed
f) Projects which could reasonably be expected to secure finance by other means

3. Application process

3.1 All applicants will be required to complete an application form and return it to the Council Offices. Electronic applications are also accepted and both this policy and the application form are available on the Town Council's website at www.marlborough-tc.gov.uk

3.2 Applicants will be required to attend the relevant Finance and Policy Committee meeting at which their application is to be considered to answer any questions, or points of clarification.

3.3 The Finance and Policy Committee will consider all grant applications at its scheduled meetings (Dates of meetings are available from the Town Council's website at www.marlborough-tc.gov.uk)

3.4 Subject to funds being available, applications will be invited throughout the year.

3.5 Deadlines for applications will normally be three weeks ahead of the meeting date.

3.6 All applicants will be contacted within two weeks of the Finance and Policy Committee's decision.

3.7 For further information about the application process or details of other local grant awarding bodies, please contact the Town Council Offices, 5 high Street, Marlborough, Wilts, SN8 1AA. Telephone: 01672 512487 or at enquiries@marlborough-tc.gov.uk.

This document is available in larger text on request

Policy reviewed by Finance and Policy Committee 30 10 23 for referral to Full Council

Proposal

Members are asked to consider the proposed amendments to the grants policy and instruct the Town Clerk accordingly.

Town Clerk 11 1 24

ITEM 8 INFORMATION MANAGEMENT POLICIES

To consider for adoption the information management policies

Purpose

The purpose of this report is to ask the Council to consider for adoption the reviewed and updated information management policies.

Background & Status

As part of the Finance and Policy Committee's review of Council polices the following have been reviewed:

Data Protection (+ separate SAR's Procedure)	Nov 2020	June 2024	Reviewed June 2023 - CH
Special Categories of Personal Data	Nov 2020	June 2024	Reviewed June 2023 - CH
Data Breach	Nov 2020	June 2024	Reviewed June 2023 - CH
Data Retention	No date	No date	Reviewed June 2023 - CH
Data Retention (appendix)	Nov 2020	No date	Updated June 2023

All policies can be found in Appendix 1

Proposal

Members are asked to consider these for adoption and instruct the Town Clerk accordingly. It is recommended that they are adopted.

Town Clerk 12 1 24

ITEM 9 COMMUNITY & YOUTH CENTRE

To consider the proposal by Wiltshire Council to asset transfer the Community & Youth Centre

Purpose

The purpose of this report is to ask Members to consider the proposal by Wiltshire Council (WC) to asset transfer the Marlborough Community and Youth Centre over to Marlborough Town Council.

Background

This matter was last considered by the Council at the Planning Committee on 25 September 2023 when this was to be considered confidentially at the request of WC. The planning Committee could not agree to proceed on this matter as requested and the following resolution was made:

RESOLVED: *to communicate to Wiltshire Council that a request to hold confidential discussions had not been carried, and seek advice on how to proceed*

The Town Clerk met the relevant WC officer at County Hall on 2 11 23 to clarify respective positions and way forward. Consequently, a letter was sent by the Town Clerk on 17 11 23 requesting an asset transfer for a nominal sum, with outline reasons and legal power specified.

Status

An email reply was received from WC Assets Team on 22 December 2023 stating:

WC have advised;

- that they are willing to explore transfer of the asset at nil value immediately on the basis of an asset transfer document for community use and an overage clause of 75% uplift on future disposal.

- The transfer document will contain a clause to set out that disposal of the site that generates value is split between the two councils. The wording will be along the lines of:

  On completion of the sale of the Disposal Land (the site) the Transferee (MTC) shall give to Wiltshire Council by way of telegraphic transfer to the Wiltshire Account 75% of the net sale proceeds (being the gross amount(s) received less solicitor fees and surveyor fees and any other costs reasonably incurred by the Transferee in effecting the sale).

i.e. after all costs of sale are removed and relates to circumstances where the town council have stopping using it for community purposes.

- For ease, WC have advised that community uses includes:

  any use which is for the benefit of the local community and/or parishioners of [PARISH] and shall include (but without limitation) cemeteries, parks, recreation areas, playgrounds, public open space, country parks, woodlands, allotments, community halls, sports pitches, sports fields, sports changing rooms and other sports facilities, toilets, affordable housing and provided that the use is ancillary to the main community use the use may also include car parking and facilities for the sale of food and drink

Considerations

This asset will become the sole responsibility of Marlborough Town Council if this proposal is accepted.

Proposal

Members are asked to consider the proposal made by Wiltshire Council and instruct the Town Clerk accordingly.

Town Clerk 11 1 24

ITEM 10 OUTSIDE BODIES

An opportunity for Members to provide verbal updates on recent interactions

ITEM 11 COMMITTEE MINUTES

In accordance with para 3.1 of the Scheme of Delegation, to note the approved minutes of the following committee meetings: **Planning** – 16 October 2023, 13 November 2023, 4 December 2023; **Amenities and Open Spaces** – 9 October 2023. These minutes have been approved by committees and circulated to Members and are available to download from https://www.marlborough-tc.gov.uk/council/meetings-agendas-minutes-from-may-2023 or from the Town Council offices. Other meetings have taken place, but minutes are not yet approved so remain in draft form.

ITEM 12 MEMBERS' QUESTION TIME

Questions to be submitted to the Town Clerk no later than noon on the day of the meeting. Not to exceed 10 minutes.

ITEM 13 COMMON SEAL

To authorise the fixing of the Common Seal of Marlborough Town Council to all documents necessary to give effect to the decisions of the meeting.

MARLBOROUGH TOWN COUNCIL

DATA PROTECTION POLICY

1. Aims

Marlborough Town Council is committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

The Town Council is registered as a data controller with the Information Commissioner.

The details of the Town Council's Data Protection Officer can be found in section 6.

2 Scope

This policy covers applies to anyone who has access to and/or is a user of Town Council ICT systems, both in and out of the Town Council, including staff, councillors, volunteers, visitors, contractors, and other community users.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3 Distribution

This policy is available on the Town Council website and in hard copy from the Town Council office.

In order to comply with the fair processing requirements of the GDPR, the Town Council informs its workforce and citizens of the data it collects processes and holds on the workforce and citizens, the purposes for which the data is held and any third parties to whom it may be passed. This information forms part of the Privacy Notice which is posted on the main Town Council website.

A paper copy of the Privacy Notice is available on request from the Town Council office. Privacy Notices are reviewed at least annually.

4 Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The Town Council may process a wide range of personal data of staff (including councillors and volunteers) and residents/citizens as part of its operation.

This personal data may include (but is not limited to):

- names and addresses (including email addresses),
- bank details,

- references,
- employment history,
- taxation and national insurance records,
- appraisal records,
- bookings (cemeteries, halls etc)
- complaints

Special category personal data - Personal data which is more sensitive and so needs more protection, including information about a living individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Criminal records are treated in much the same way as other special category data

Processing - Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject - The identified or identifiable (living) individual whose personal data is held or processed.

Data controller - A person or organisation that determines the purposes and the means of processing of personal data.

Data processor - A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5 Roles and Responsibilities

This policy applies to all staff (including volunteers and councillors) who work at the Town Council, and to external organisations or individuals working on its behalf.

Councillors - The Councillors has overall responsibility for ensuring that the Town Council complies with all relevant data protection obligations.

Town Clerk - The Town Clerk acts with the delegated authority of the Full Council on a day-to-day basis and will liaise with the DPO. In the Town Clerk's absence, in case of emergency, this role will be delegated to the Assistant Town Clerk.

All staff - All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff; The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting data in line with this policy and the retention schedule
- Informing the Town Council of any changes to their personal data, such as a change of address
- Reporting to the Town Clerk, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and page 9 of this policy.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to likely to be required please see - *Sharing Personal Data* (section 10)

6 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing

related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the Council and, where relevant, provide the Town Council with advice and recommendations on data protection issues.

The Town Council has appointed i-West as its DPO and they can be contacted by email at

Email: i-west@bathnes.gov.uk.

Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the Town Clerk or the Assistant Town Clerk will be the point of contact with the DPO.

7 Subject Access Requests and Other Rights of Individuals

In all aspects of its work, the Town Council will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Town Council's work. Subject to exceptions, the rights of the data subject as defined in law are;

a) The Right to be informed.

The Town Council advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation such as consent forms where appropriate.

b) The Right of access

An individual when making a subject access request (SAR) is entitled to the following;

i. confirmation that their data is being processed;
ii. access to their personal data;
iii. other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

The Town Council must respond to such a request within 30 days unless the request is complex, in which case it may be extended by a further 60 days. Please refer to Appendix 1 for further details as to how to manage a subject access request.

c) The Right to rectification

Individuals have the right to ask to rectify information that they think is inaccurate or incomplete. The Town Council has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified.

d) The Right to erasure

The right for an individual to request that their data is erased is not absolute. It applies where:

- the information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- the information is no longer required by the Town Council;
- a legal obligation to erase the data applies;
- the data was collected from a child for an online service;
- the Town Council has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the Town Council to continue to process it.

e) The Right to restrict processing

An individual may ask the Town Council to temporarily limit the use of their data when it is considering:

- a challenge made to the accuracy of their data, or
- an objection to the use of their data.

In addition, the Town Council may be asked to limit the use of data rather than delete it, if the individual does not want the Town Council to delete the data but does not wish to it continue to use it, in the event that the data was processed without a lawful basis or to create, exercise or defend legal claims.- .

f) The Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The Town Council only has to provide the information where electronically feasible.

g) The Right to object

Individuals have a right to object in relation to the processing of data for

- a task carried out in the public interest
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or

- direct marketing.

h) The right to withdraw consent to processing

i) Rights related to automated decision making

This does not apply as the Town Council does not employ automated decision making processes.

8 Data Protection Principles

The GDPR is based on 7 key data protection principles that the Town Council complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the Town Council will explain to individuals why the Town Council needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The Town Council reviews its documentation and the basis for processing data on a regular basis.

- **Collected for specified, explicit and legitimate purposes** – the Town Council explains these reasons to the individuals concerned when it first collects their data. If the Town Council wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ The Town Council will document the basis for processing. For special categories of personal data, it will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** the Town Council must only process the minimum amount of personal data that is necessary in order to undertake its work.

- **Accurate and, where necessary, kept up to date** – the Town Council will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

- **Kept for no longer than is necessary for the purposes for which it is processed** – when the Town Council no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule.

- **Processed in a way that ensures it is appropriately secure** – the Town Council implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy for further information which incorporates principles around Bringing Your own Device (BYOD), the Town Council's remote access policy, and how data is securely transferred in and out of the Town Council's system.

- **Accountability –** The Town Council complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:

  - Completing Data Protection Impact Assessments (DPIAs) where the Town Council's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the Town Council will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
  - Integrating data protection into internal documents including this policy, any related policies and Privacy Notices;
  - Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the Town Council also maintains a record of attendance;
  - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and Town Council policies;
  - Maintaining records of its processing activities for all personal data that it holds.

9 Processing Personal Data

In order to ensure that the Town Council's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- The data needs to be processed so that the Town Council can fulfil a **contract** with the individual, or the individual has asked the Town Council to take specific steps before entering into a contract;
- The data needs to be processed so that the Town Council can comply with a **legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;
- The data needs to be processed so that the Town Council, as a public authority, can **perform a task in the public interest, and carry out its official functions**;
- The data needs to be processed for the **legitimate interests** of the Town Council or a third party where necessary, balancing the rights of freedoms of the individual).

However, where the Town Council can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** The Town Council will seek consent to process data from the child depending on their age and capacity to understand what is being asked for.

For processing special categories of personal data an additional lawful basis is needed – these are detailed in the Special Categories of Personal Data Policy.

10 Sharing Personal Data

Please refer to the Town Council's Privacy Notices.

- The Town Council will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:
  - The Town Council will share data if there is an issue with a child or parent/carer that puts the safety of staff at risk;
  - The Town Council will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or child;
  - The Town Council's suppliers and contractors need data to provide services – for example, IT companies. When sharing data the Town Council will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares where there is regular sharing ;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Town Council.
- The Town Council may also share personal data with law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:
  - For the prevention or detection of crime and/or fraud;
  - For the apprehension or prosecution of offenders;
  - For the assessment or collection of tax owed to HMRC;
  - In connection with legal proceedings;
  - For research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

- The Town Council may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects councillors or staff.

11 Data Protection by Design and Default

The Town Council has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity i-west must be consulted and an initial screening be conducted assessing risk.

Please refer to the Information Security Policy for further detail as to how the Town Council implements this principle in practice.

12 Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Town Clerk and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

13 Destruction of records

We apply our retention policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.

We will securely destroy hard copies and will ensure that any third party who is employed to perform this function will have the necessary accreditations and safeguards.

If we delete electronic records and our intention is to put them beyond use, although it may be technically possible to retrieve them, we follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

14 Training

To meet our obligations under Data Protection legislation, we ensure that all staff, volunteers, and councillors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it, for example relating to use of systems or as appropriate.

Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the Town Council's processes make it necessary.

15 Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Town Council's overall compliance with data protection law, the Town Council is responsible for the day-to-day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the Town Council's ability to comply with this policy and the legislation.

This policy will be reviewed annually, unless an incident or change to regulations dictates a sooner review.

16 Complaints

The Town Council is always seeking to implement best practice and strives for the highest standards. The Town Council operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Town Council's complaints policy may be found on its website.

You have a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the Town Council or via the Town Council's DPO.

The ICO is contactable at;

Wycliffe House, Water Lane,
Wilmslow, Cheshire,
SK9 5AF.

Telephone: 0303 123 1113.

18 Legislation and Guidance

This policy takes into account the following:

- The General Data Protection Regulation (GDPR) 2016
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office

19 Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Data Retention Policy
- Special Categories of Personal Data Policy
- Data Breach Policy
- Privacy Notices
- Safeguarding Policy
- Acceptable Usage Policies
- Consent / Permissions Form

20 Document change history

Date	Changes made
Sept 2020	Policy revised
Nov 2020	Adopted by Full Council
June 2023	Reviewed

Appendix 1 – Subject Access Request Procedure (SAR)

The Town Council shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west), using the Town Council SAR Guidance provided to the Town Council.

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the Town Council.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (i-west), and their Town Council SAR Guidance.

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.

Marlborough Town Council

Subject Access Request Procedure (SAR)

The Town Council shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (OneWest), using the Town Council SAR Guidance provided to the Town Council.

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with:
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to the Town Council.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (OneWest), and their Town Council SAR Guidance.

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.

Reviewed 8th August 2023

MARLBOROUGH TOWN COUNCIL

SPECIAL CATEGORIES OF PERSONAL DATA POLICY AND CRIMINAL OFFENCES DATA POLICY

1. Introduction

The Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR) require a policy document to be in place where special category data or criminal offence data are being processed under certain grounds.

The law puts in place extra protections for special category data and criminal convictions because of their sensitivity. This document explains how Marlborough Town Council meets these requirements when:

a) Processing special category data on the grounds of substantial public interest; or
b) Processing special category data for the purposes of carrying out the obligations and exercising specific rights under employment and social security and social protection law; or
c) Where criminal offence data is being processed.

2. Scope

This policy applies to all employees of Marlborough Town Council including contract, agency and temporary staff, volunteers, councillors and employees of partner organisations working for the Town Council.

In this policy we refer to the "individual." By this we mean the data subject i.e. the identified or identifiable living individual to whom personal data relates.

3. What are Special Categories of Personal Data?

The categories of data within scope of this policy are personal data revealing an individual's:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health; or
h) data concerning a natural person's sex life or sexual orientation.

Adopted by Full Council – November 2020
Reviewed – June 2023

4. Legal Basis for processing special category data

In order to process **any** personal data about an individual, we must **firstly** satisfy one of the grounds for processing personal data under Article 6 of the GDPR. In certain circumstances, Schedule 1 of the Data Protection Act must also be complied with. These grounds are:

- Consent – the individual has given clear consent for their data to be processed for a specific purpose
- Contract – the processing is necessary for a contract we have with the individual, or because the individual has asked us to take specific steps before entering into a contract
- Legal obligation – the processing is necessary for us to comply with the law
- Vital interests – the processing is necessary to protect someone's life
- Public task – the processing is necessary for us to perform a task in the public interest, or for its official functions and the task or function has a clear basis in law
- Legitimate interests – the processing is necessary for our legitimate interest or the legitimate interests of a third party, unless the interests of the individual override the the Town Council's interests. However, this ground does not apply to a public body for delivering its statutory responsibilities, such as us, where we may rely on the public task ground instead.

In addition to the legal basis to process personal data, special categories of personal data also require an additional legal basis for processing under Article 9 of the GDPR. These grounds are as follows:

a) The individual has given **explicit consent** to the processing of those personal data for one or more specified purposes.

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

Health or social care purposes includes the following purposes-

i. Preventative or occupational medicine
ii The assessment of the working capacity of the employee

c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the

processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals concerned.

e) Processing relates to personal data which are **manifestly made public by the individual**

f) Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity

g) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

h) Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

i) Processing is necessary for reasons of **public interest in the area of public health**

j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest as follows:

- Schedule 1, Part 1 of the Data Protection Act 2018 which provides that processing under points (b), (h), (i) or (j) of the GDPR above (conditions relating to employment, health and research).

- Schedule 1, Part 2 of the Data Protection Act 2018 in respect of point (g) above (substantial public interest)

The Schedules can be found in the Data Protection 2018 and further define the grounds thereby offering further protections. This policy satisfies the requirements of the Schedule.

Our Privacy Notice, which may be found on our website, sets out the types of special category data that we process.

5. Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

Whenever we process criminal offence data, we satisfy one of the lawful basis processing under Article 6 of the GDPR (as per paragraph 4 above), Article 10 of the GDPR and a condition under Schedule 1 of the Data Protection Act 2018.

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection or

- Consent –where freely given. We acknowledge because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid, and will only rely on this where no other ground applies.

6. How Marlborough Town Council meets the principles of the GDPR

Article 5 of the GDPR sets out the data protection principles. Below follow our procedures for ensuring that we comply with the principles when we are processing special category or criminal data:

Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner.

- We ensure that personal data will only be processed where a lawful basis applies and where processing is otherwise lawful;
- We only process personal data fairly and ensure that individuals are not misled. We publish our privacy notice on our website and keep it up to date. Where there have been significant changes, we will do what is reasonable to advise individuals of the changes;

- We ensure that wherever consent is sought from individuals to process their data, that it is freely given, specific, informed and unambiguous of the individual's wishes.
- Where we are processing criminal offence data, as part of our employment duties, our policies are clear to applicants in terms of what we do with their data, how it is taken into account and whether it is retained.

Principle 2 – Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes:

- We will not use personal data for purposes that are incompatible with the purposes for which it was collected. If we use personal data for a new purpose that is compatible with the original, we will ensure that there is a lawful basis upon which the data can be processed.

  In deciding whether a purpose is compatible, in accordance with the guidance from the Information Commissioner's Office, we will take into account the following:

  - Any link between the original and new purpose
  - The context in which the original data was collected
  - The nature of the personal data – how sensitive is it?
  - The possible consequences to the individual
  - Whether appropriate safeguards are used – for example encryption, pseudonymisation.

    The following purposes are stated by the GDPR to be compatible:
    - Archiving in the public interest
    - Scientific or historic research purposes
    - Statistical purposes.

- In appropriate cases, including where consent formed the original basis for processing, we will seek the individual's explicit consent to use the data in a way that was not originally envisaged.

Principle 3 – Personal data will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

- We will only collect the minimum personal data that we need for the purpose for which it is collected.

Principle 4 – Personal data will be accurate and where necessary kept up to date.

- We will take particular care to do all that is reasonable to ensure the accuracy of the information where it has a significant effect on individuals.
- At appropriate intervals, we will remind individuals, workforce/citizens of the need to ensure that the data that they provide is accurate and up to date. When we are advised of changes, we will ensure that our records are updated as soon as is practicable.

Adopted by Full Council – November 2020
Reviewed – June 2023

- We review requests to have data erased or rectified as soon as possible, and usually within 30 days. We rectify inaccurate data.

Principle 5 – Personal data should be kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the personal data is processed:

- We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
- We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities or sooner if needed;
- We have a retention and disposal policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
- Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.
- We do not retain DBS certificates for longer than 6 months.

Principle 6 – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Extra care is taken with special category and criminal offence data;

a) We adopt a risk based approach to taking data offsite. Unless absolutely necessary, hard copies of sensitive personal data will not be removed from our premises.

   Any decision to remove the information must be based on the business need of the Town Council or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any sensitive data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.

   If there is no reasonable alternative to removing hard copies from the Town Council offices, the following procedure will apply:

   i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed;
   ii. Information will be transported and stored in a lockable case;
   iii. Wherever possible, information that is removed from site will be pseudonymised by using a “key” held by the office on site;

iv. We adopt a risk- based approach, for example hard copy personal data with lower sensitivity (e.g. marketing lists) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. HR, Safeguarding, Health data) must be kept on the staff member's person at all times.

v. Sensitive personal data must be returned to the Town Council's premises at the end of the working day. If this is not practicable, and a staff member needs to retain the information in their personal possession, this must be discussed in advance with the Town Clerk including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The Town Clerk must record their decision.

b) Data will be tidied away when not in use (e.g. when staff undertake work at home, it must be out of sight of family members, not left out and tidied away afterwards).
c) Only those who have need to access the data concerned will be granted permission and access to it.
d) Our data security policy / acceptable use / remote working policies describe the requirements around bring your own device, remote working and password protection.

Principle 7 - Accountability

In addition, to complying with the principles above, we are required to demonstrate how we evidence our compliance with them.

The ways in which we do so include:

i) Data Protection Impact Assessments (DPIA)

It is a statutory requirement that any processing of personal data which may result in a high risk to the data protection rights of the individual be assessed by means of a Data Protection Impact Assessment.

Even though a DPIA may be required in other circumstances, examples of high risk activities include:

- Processing of special category data or criminal convictions on a large scale
- Systematic monitoring of a publicly accessible area on a large scale
- Automated decision making with legal or similar significant effect

Prior to the assumption of any such activity, we will consult with the Data Protection Officer to assess risks based on an initial screening process. If required, a full DPIA will be

undertaken to determine whether this activity should proceed. We keep DPIA's under review, and will revisit them in the event of significant changes.

The DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

ii) Those staff members handling data and in particular special category data will be trained in how to handle it, to an appropriate standard. This may include additional training on systems that handle sensitive personal data, which will be undertaken before the member of staff has full access to the system. Records will be maintained of the training undertaken.

iii) Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated in accordance with new guidance, legislation and practice. They will be publicised to staff who will be required to familiarise themselves with them.

iv) The Record of Processing Activities will be maintained and reviewed at least annually;

v) Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate; and

vi) Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer and/or a Risk Register.

7. Monitoring and compliance

This policy will be reviewed annually, unless a change to legislation, practice or incident require a sooner review.

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to Town Clerk and/or Councillors.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Adopted by Full Council – November 2020
Reviewed – June 2023

MARLBOROUGH TOWN COUNCIL

DATA BREACH POLICY

1. Introduction

Marlborough Town Council issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach is defined as the compromise of information's confidentiality, integrity, or availability which may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Scope

This policy applies to all employees of Marlborough Town Council including contract, agency and temporary staff, councillors, volunteers and employees of partner organisations working for the Town Council.

3. Data Breaches

For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked

- Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

4. Reporting

The quick response to a suspected or actual data breach is key. All consumers in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours then this should be reported as soon as practically possible. This should be done through the completion of the reporting form in Appendix 1, which is sent to the Town Clerk who will liaise with its Data Protection Officer (i-west).

5. Security Incident Management (SIM)

The organisation's lead officer shall complete the following phases of SIM (which are detailed in Appendix 2) with advice from its Data Protection Officer:

a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches

b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.

c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.

d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.

e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. The organisation's Communications / Press Team may also be notified to handle any queries and release statements.

A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Whether policy controls are sufficient

- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary

If necessary a report recommending any changes to systems, policies and procedures will be considered by the senior management board. This will include the decision on whether to report to the regulator and affected data subjects.

Phases (b) to (e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported.

6. Monitoring and compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;

Change of Data Protection Officer,

Change of Legislation

Appendix 1 – Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	

Appendix 2 - Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• IT Support provided by Excalibur • DPO provided by i-West • The Record of Processing Activities (RoPA) will provide details of data, flows, owners, custodians, and third parties – link to the RoPA • GDPR Training rolled out to staff
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	

6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	
	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned **Decision to report to ICO** - Yes / No Based on: Officer: Signed: Date:

MARLBOROUGH TOWN COUNCIL

DATA RETENTION POLICY

1. Introduction

Marlborough Town Council issues this policy to meet the requirements incumbent upon them under The GDPR and the Data Protection Act 2018 for the handling of personal data in its role as a data controller.

2. Scope

This policy applies to all employees of Marlborough Town Council including contract, agency and temporary staff, volunteers, councillors and employees of partner organisations working for the Town Council.

3. Retention

In line with the GDPR and the Data Protection Act 2018, the organisation will keep some forms of information for longer than others. Information will not be kept indefinitely unless there are specific requirements.

Appendix A gives a detailed breakdown of timescales for the retention of various types of information.

4. Disposal

When data is no longer required it should be appropriately destroyed. A log will be maintained summarising the information which has been disposed of.

The organisation will either use an accredited confidential waste disposal provider, or it will shred the information to using a cross-cut shredder. Information on what should be deemed as confidential waste is detailed in **Appendix 1**.

5. Monitoring and compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the Town Clerk.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with the Town Clerk, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;
Change of Data Protection Officer
Change of Legislation

Appendix 1 - What is Confidential Waste?

(1) Any record* which details <u>personal</u> information

What is personal information?

- Relates to and identifies a living person
- Could help someone identify a person when used with other information
- Is an expression of opinion about an individual
- Indicates our intentions towards an individual

Such as: Name, Address, Date of Birth, Email, Phone numbers, Location data, IP addresses

(2) Any record* which details <u>special categories of personal data</u>

What is special categories of personal data?

- Racial and/or Ethnic Origin
- Political Opinions
- Religious Beliefs (or other beliefs of a similar nature)
- Trade Union membership
- Biometric Information e.g. Photos
- Mental or Physical Health condition
- Sexual life and Orientation
- Criminal Records (actual or suspected)

Such as: Safeguarding, Accident/First Aid, Equalities information, Legal records

(3) Any record* which details <u>business/commercially sensitive</u> information

What is business/commercially sensitive information?

- Information which Marlborough Town Council would be affected by any loss of, or unauthorised access to.

Such as: Contracts, opinions on service delivery, tender information.

If you have any doubt then please treat the information as Confidential

***** *A Record can be in many formats – e.g. Paper, Post-it notes, Disks, CDs, Tapes, Posters etc.*

Marlborough Town Council

Appendix A – List of documents for retention/disposal

Description	Legal Basis	Retention Period	Action upon Expiry	Potentially contains SC data	Protectively Marked	Notes
Council						
Register of Member's addresses	Legitimate interests	Date of next election +2 years	Secure disposal	No	Not Protectively Marked	
Allowance Information	Income Tax (PAYE) Regulations 2003, reg 97	Not less than 3 years after the end of the tax year to which they relate	Secure disposal	No	Confidential	
Meetings						
Signed minutes	Local Government Act 1972 sch.12(19)	Date of meeting + 8 years	Permanent preservation	No	Not Protectively Marked	
Minute taker notes	Legitimate interests	Until transposed	Secure disposal	No	Not Protectively Marked	
Accounting						
Cashbook & account book reconciliations	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	No	Not Protectively Marked	Financial sensitive

Revised 8th August 2023

Marlborough Town Council

Paid Invoices	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	Yes	Not Protectively Marked	Financial sensitive
Paying in books	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	Yes	Not Protectively Marked	Financial sensitive
Cash receipt book	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	No	Not Protectively Marked	Financial sensitive
Payroll records	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	Yes	Confidential	Financial sensitive
Bank statements	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	Yes	Not Protectively Marked	Financial sensitive
Cheque stubs	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	Yes	Not Protectively Marked	Financial sensitive

Revised 8th August 2023

Marlborough Town Council

Investment Management						
Investment records	Legitimate Interests (Audit)	Indefinitely	Permanent preservation	No	Not Protectively Marked	Financial sensitive
Annual Accounts						
Annual accounts closure records	Legitimate Interests (Audit)	Indefinitely	Permanent preservation	No	Not Protectively Marked	Financial sensitive
VAT						
VAT records	HMRC-Compliance Handbook Manual CH15400	Financial year + 6 years	Secure storage	No	Not Protectively Marked	Financial sensitive
Employee Information						
Records relating to employment history to include contracts, training etc.	Limitation Act 1980 s.5	6 years after cessation of employment	Secure storage	Yes	Confidential	`
Salary information (tax & NI)	Income Tax (Pay As You Earn) Regulations 2003, reg 97	3 years after the end of each tax year	Secure storage	Yes	Confidential	Financial sensitive
Staff pension contributions records	The Retirement Benefits Schemes (Information Powers) Regulations 1995 s.15	End of scheme + 6 years	Secure storage	Yes	Confidential	Financial sensitive

Revised 8th August 2023

Marlborough Town Council

Timesheets	The Working Time Regulations 1998, Part II	2 years after creation date	Secure disposal	Yes	Confidential	
Application & CV for successful candidates	Limitation Act 1980 s.5	6 years after cessation of employment	Secure disposal	Yes	Confidential	
Application & CV for unsuccessful candidates	ICO Employment Practices Code para 1.7	6 months after position filled or vacancy closed	Secure disposal	Yes	Confidential	
Correspondence						
Emails & general correspondence	Legitimate interests	1 Year	Secure disposal	Yes	Not Protectively Marked	
Audit (internal & external)						
Internal Audit Report	Local Audit and Accountability Act 2014	Permanent	Permanent preservation	No	Not Protectively Marked	Financial/business sensitive
External Audit Report + all supporting documents	Local Audit and Accountability Act 2014	Permanent	Permanent preservation	No	Not Protectively Marked	Financial/business sensitive
Records of Contracts and Tenders						
Quotes	Legitimate interests	1 year after the end of the tender process	Secure disposal	No	Not Protectively Marked	Financial/business sensitive

Revised 8th August 2023

Marlborough Town Council

Unsuccessful tenders	Legitimate interests	1 year after the end of the tender process	Secure disposal	No	Not Protectively Marked	Financial/business sensitive
Successful tenders	Limitation Act 1980 s.5	6 years after end of contract	Secure disposal	No	Not Protectively Marked	Financial/business sensitive
Signed contracts	Limitation Act 1980 s.5	6 years after end of contract	Secure disposal	No	Not Protectively Marked	Financial/business sensitive
Insurance Policies						
Employer's Liability and Public Liability Insurance policies	The Employers' Liability (Compulsory Insurance) Regulations 1998	While valid	Disposal	No	Not Protectively Marked	Financial sensitive
General Properties						
Deeds of title	Legitimate interests	Permanent	Permanent preservation	No	Not Protectively Marked	Financial/business sensitive
Searches and surveys	Legitimate interests	Permanent	Permanent preservation	No	Not Protectively Marked	Financial/business sensitive
Leases	Legitimate interests	Permanent	Permanent preservation	No	Not Protectively Marked	Financial/business sensitive
Town Hall, MC&YC, Recreation Ground and Open Spaces						

Revised 8th August 2023

Marlborough Town Council

All hirer booking forms, lettings diaries, copies of invoices etc	Legitimate interests	Current Council term + 4 years	Secure disposal	Yes	Not Protectively Marked	
Allotments						
All records relating to allotment holders	Legitimate interests	Tenure of plot	Secure disposal	Yes	Confidential	
Legal documentation/ register & plans	Legitimate interests	Permanent	Permanent preservation	No	Not Protectively Marked	
Burial Grounds						
Register of fees, burials, purchased graves & memorials. Applications for interment, rights to erect memorials, disposal certificates, copy certificates of grants of exclusive rights of burial & burial plan	Local Authorities' Cemeteries Order 1977	Permanent	Permanent Preservation	Yes	Confidential	

Revised 8th August 2023