

## Finance and General Purposes Committee Meeting

Kidsgrove Town Council  
Victoria Hall  
Liverpool Road  
Kidsgrove  
Staffordshire  
ST7 4EL

Tel: 01782 782254

[www.kidsgrovetowncouncil.gov.uk](http://www.kidsgrovetowncouncil.gov.uk)



13<sup>th</sup> March 2019

To: Members of the F&GP Committee of Kidsgrove Town Council

Dear Councillor,

You are summoned to attend the meeting of Kidsgrove Town Council, Finance and General Purposes Committee to be held at 7.15pm on Monday 18<sup>th</sup> March, at Kidsgrove Town Council (Chairman's Room).

Yours sincerely,

Sue Davies  
Town Clerk

### Business to be transacted

- 1) To receive and consider apologies for absence
- 2) To note declarations of Members' Interests
- 3) To consider and approve the minutes of the meeting of 14<sup>th</sup> February 2019 (Appendix 1).
- 4) Public Participation

A period not exceeding 15 minutes for members of the public to ask questions or submit comments. (No individual to speak for more than 2 minutes without the permission of the chair.)

- 5) Matters arising not covered elsewhere on the agenda:
  - a. Five-year plan meeting: To note the date has been set as the 4<sup>th</sup> April 2019, 19:00, Chairman's Room
  - b. Unity Bank application progress: to receive an update from the Clerk
  - c. National Savings Account update from the Clerk
  - d. Barclays Accounts Closure – to receive an update from the Clerk.
  - e. Kitchen update – deep clean
- 6) To receive the results of the external audit 2017/2018 (See appendix 2) and to resolve to agree any recommendations to Full Council.

- 7) GPPR – To receive the draft GDPR review report from the Data Protection Officer, JDS Business Services and agree any comment prior to the issue of the final report. (See appendix 3)
- 8) To receive a first draft of a revised Risk Assessment document for initial comment. (Circulated separately).
- 9) To receive and comment on a draft grant application policy and application form and to recommend approval to Full Council subject to any agreed changes. (Circulated separately.)
- 10) To receive a verbal update from the Clerk on matters relating to the Victoria Hall including:
  - a. Handover matters from Newcastle under Lyme Borough Council: To receive an update from the Clerk.
  - b. To consider and agree any actions required regarding the door access arrangements into the bar area.
  - c. Repairs to tables in the Chairman’s room – to consider and agree any actions required.
  - d. To receive a report from the Clerk on the review of Health and Safety Matters by Ellis Whittam and to agree any actions recommended by the Clerk.
  - e. To receive and approve the Terms of Reference for the bar contract working group. (See appendix 4).

Note – Further matters relating to the Victoria Hall are considered in Part 2.

- 11) Council Finances: To receive a list of payments to be made and requiring approval from the RFO (invoices and payroll will be available at the meeting).
- 12) To receive a verbal report from Cllr Cooper regarding the Dementia Friendly Initiative and to note the two sessions that have been organised at the Town Hall.
- 13) Key Future Agenda items:

Revision of booking forms and issue of guidelines.
- 14) To agree the date and time of the next meeting: Tuesday, 9<sup>th</sup> April 2019, 19:00.

### **Matters to be considered with the Press and Public Excluded:**

- 15) Exclusion of press and public: To resolve under 1960 (Admission to meetings) Act to exclude the press and public due to the confidential nature of the business to be discussed.
- 16) Bar Contract:
  - a. To receive the minutes of the bar contract working group from the meetings of the 19<sup>th</sup> February and 5<sup>th</sup> March 2019. (Circulated separately)
  - b. To receive and consider a report from the bar contract working group and to agree the recommendations subject to any agreed changes. (Circulated separately).
- 17) Staffing Matters: To receive a verbal report from the chair of the staffing committee on relevant matters to the F&GP Committee arising from the Staffing Committee meeting which immediately preceded the F&GP Committee Meeting.
- 18) Town Council Victoria Hall Contracts: To receive a written report from the Clerk and to agree any recommendations to full council:
  - a) Security Contract. (Circulated separately)
  - b) Caretaking of the Victoria Hall. (Circulated separately)
  - c) Cleaning Contract. (Circulated separately)

## Finance and General Purposes Meeting

Kidsgrove Town Council  
Victoria Hall  
Liverpool Road  
Kidsgrove  
Staffordshire  
ST7 4EL

Tel: 01782 782254

[www.kidsgrovetowncouncil.gov.uk](http://www.kidsgrovetowncouncil.gov.uk)



### Minutes of the Finance and General Purposes Committee meeting held 14<sup>th</sup> February 2019, 7:00pm, Chairman's Room, Victoria Hall

- FPG/18-19/3/1** Present
- Cllr A Cooper (Chair), Cllr S Dymond, Cllr M Stubbs, Cllr P Waring, Cllr A Cartwright, Cllr J Dodgson, Cllr S Bowyer  
In attendance: Sue Davies, Town Clerk  
Cllr V Jukes attended as a member of the public.
- FPG/18-19/3/2** To receive and consider apologies for absence
- No apologies were received.
- FPG/18-19/3/3** To note declarations of Member's Interests
- None declared.
- FPG/18-19/3/4** To consider and approve the minutes of the Finance and General Purposes Committee meeting held on the 15<sup>th</sup> January 2019
- The minutes of the meeting of the Finance and General Purposes Committee meeting held on the 15<sup>th</sup> January were approved and signed as an accurate record.
- FPG/18-19/3/5** Public Participation (A period of not exceeding 15 minutes for the press or public to make comments.)
- No comments made.
- FPG/18-19/3/6** Matters Arising
- a) Bar Contract – an update**
- The Clerk reported that the first meeting of the Task Group set up to consider the bar contract would be meeting on the 19<sup>th</sup> February 2019.
- b) Kitchen Update – deep clean**
- The Clerk reported that quotes are currently being received for a deep clean.

Chairman's Initials.....  
Kidsgrove Town Council

**FPG/18-19/3/7**

To consider and agree to recommend to Full Council draft Terms of reference for the F&GP Committee.

The draft Terms of Reference were considered.

It was resolved to recommend approval to full council with the following changes:

- Membership be fixed at seven councillors.
- It should be clear that the council can only strive to ensure each political faction and ward is represented and the wording should reflect this.
- That the delegated power to set up working parties and sub-committees should be made clear to only apply to items under the delegated power of the committee.

The Terms of Reference agreed are shown in appendix 1.

**FPG/18-19/3/8**

To Receive an update from the Clerk on the interim internal audit held on the 7<sup>th</sup> February 2019.

The Clerk presented the results of the Interim Internal Audit and circulated paper copies that had been received that day.

The key issues raised were:

- Inadequate administration to support authorisation of payments. The Clerk is already looking to improve the system of authorisation of payments.
- Review of the activity on the unused bank accounts.
- Lack of Terms of Reference for the FGP Committee – Now being put in place.
- No paperwork to support the bar commission payment.
- Poor filing of sales invoicing and no clear strategy for the granting of concessions. The clerk is to draft a policy.

**FPG/18-19/3/9**

Bank Accounts and Approval of Payments

The Committee received a report from the Clerk (FGP-18/19-03) and **resolved** to recommend the following to Full Council for approval:

- That a Unity Bank Account be opened to work alongside the current Barclays Bank Account.
- That a Unity Bank credit card be applied for with a payment limit of 500 pounds.
- That the two Barclays accounts which are currently unused are shut but that the mayor's charity account is kept open for that very purpose.
- That once the Unity Account is open, that the Clerk redraft the financial regulations to reflect the new authorisation process.

**FPG/18-19/3/10**

Five-Year Plan

The mechanism of forwarding the 5-year plan was debated. It was resolved to recommend to Full Council that the Clerk pull together the results of the initial 'brain storming' sessions held by

councillors and that a further meeting be organised to which all councillors be invited to discuss the priorities and way forward.

*The Chair suspending Standing Orders to allow Cllr Jukes to speak.*

Cllr Jukes asserted his opinion that the plan should ensure that each ward is fairly represented.

**FPG/18-19/3/11** Risk Assessment Document

The Clerk informed that she would draft a Risk Assessment prior to the next meeting for review and comment before bringing a draft to the next FGP Committee meeting.

**FPG/18-19/3/12** To receive an application from Kidsgrove Scouts for funding support and to consider a recommendation to Full Council.

An application from Kidsgrove Scouts was considered. It was agreed that further information was required before the application could be fully considered and that the matter should be referred to the next FGP Committee before going to Full Council in March.

It was also identified that the Council need a clear and transparent grant awarding policy.

*Action: The Clerk to contact the Scouts to request more information and to draft a grant awarding policy.*

**FPG/18-19/3/13** To receive a Verbal Update on Matters relating to the Victoria Hall.

The Clerk updated the Council regarding matters relating to the Victoria Hall. In particular, there has been in a leak in the refreshments room which requires attention.

**FPG/18-19/3/14** To note the date of the next meeting.

Monday, 18<sup>th</sup> March 2019

The meeting concluded at 21:15pm

# Kidsgrove Town Council

Kidsgrove Town Council  
Victoria Hall  
Liverpool Road  
Kidsgrove  
Staffordshire  
ST7 4EL

Tel: 01782 782254  
[www.kidsgrovetowncouncil.gov.uk](http://www.kidsgrovetowncouncil.gov.uk)



## Finance and General Purposes Committee Terms of Reference.

### 1) Introduction

The Finance and General Purposes Committee is set up as a standing committee to oversee and manage Kidsgrove Town Council's finances and other matters of Council business. Unless it has delegated authority, the committee will propose recommendations to Full Council as required.

The Committee was set up by Kidsgrove Town Council at its meeting of 16<sup>th</sup> August 2018 (minute reference 18/3/06).

The Committee must always abide with the Council's current approved Standing Orders and Financial Regulations.

The membership of the Committee for each Council year and a review of the Terms of Reference will be agreed at each Annual Meeting of the Full Council. The chair and vice-chair will be elected at the first meeting of the Committee following the Annual Meeting.

### 2) Membership

The Committee will consist of seven Councillors with a quorum for a meeting being three Councillors. The Mayor and Deputy Mayor will be members ex-officio. Each political faction and each ward of the council should be represented whenever possible.

The Committee can only consist of Kidsgrove Town Council Members.

### 3) Aim and Remit of the Finance and General Purposes Committee

#### a) Financial Aspects

- i) Working with the RFO, to manage the Council's finances and to ensure that proper practices are maintained.
- ii) Working with the RFO, to manage and monitor performance against the current year's budget and to make recommendations for action when necessary.<sup>1</sup>

---

<sup>1</sup> Note – budgetary matters including precept requirements cannot legally be delegated to a committee and all decisions must always strictly remain with the Full Council.

- iii) Working the RFO, to consider budgets for the following financial year, receiving reports from the Council's other Committees as required, and to put a recommendation to Council for approval.
  - iv) To recommend to Full Council the precept requirements for the following year in a timely manner to allow the precept to be submitted to Newcastle-under-Lyme Borough Council by their deadline.
  - v) Working with the RFO, to manage the forecasts of the Council's finances over the next five years, ensuring appropriate approvals are received from Full Council at timely intervals in line with the five-year plan including managing the council's reserves.
  - vi) Working with the RFO, to ensure appropriate financial risk assessments are in place.
  - vii) To review insurance a least annually and to make recommendations to full Council.
  - viii) To oversee and manage the Council's financial affairs in relation to business activities including the VAT implications to the Council.<sup>2</sup>
  - ix) To oversee the Council's contracts, putting recommendations to Full Council.
  - x) To ensure an up to date asset register is maintained by the Council. To ensure the asset register is approved by Full Council at least annually and after any changes perceived by the committee to be significant. The RFO will present an asset register update at least bi-annually to committee.
  - xi) To review internal and external audits and to make recommendations to Council when required to ensure all points raised are addressed.
  - xii) To manage the Council's own 'in-house' checks on financial procedures, ensuring member checks occur appropriately throughout the year and are documented and reported to Full Council with recommendations if required.
  - xiii) To consider applications for grants received by the Council in line with the council's grant application policy.
  - xiv) To pursue potential funding opportunities.
- b) General Purposes Remit
- i) To manage Town Council affairs and issues which are not specifically under the remit of another committee.
  - ii) To consider and manage the Town Council's Policies and Procedures prior to approval at Full Council.<sup>3</sup>

---

<sup>2</sup> Business Activities relate to the hiring out of the Victoria Hall and other rooms and the management of the bar.

<sup>3</sup> Policies and Procedures may be taken directly to Full Council on occasion, at the Clerk's discretion, to allow timely issue.

- iii) To manage the progression of the Council’s five-year plan and to ensure progression updates and recommendations are put to Full Council for approval as required.
- iv) To manage the Victoria Hall Building including:
  - (1) Health and safety requirements
  - (2) Maintenance
  - (3) Contracts
  - (4) Licences
- v) To manage any aspects of the Town Council’s business which isn’t covered by the Terms of Reference of another Committee.
- vi) To ensure Members of the Committee receive appropriate and adequate training to provide understanding of Local Council Finance and Governance.

#### **4) Delegated Powers of the Committee**

The Committee can make decisions only within that allowed in the current versions of approved Standing Orders, Financial Regulations and the powers delegated to it by the Council which are listed below:

- a) To approve schedules of payments presented by the Clerk/RFO, including payroll. Schedules approved for payment by the FGP Committee should be listed at the next Full Council Meeting.
- b) To authorise expenditure on behalf of the Council for all budgeted monies up to the limit contained in the version of the Financial Regulations current at that time.<sup>4</sup>
- c) To authorise grants submitted to the Council up to the limit specified in the grants policy and in line with item 4(b).
- d) To be able to apply for funding and grants in the Town Council’s name without approval by Full Council although such actions should be reported at the next Full Council meeting.
- e) To be able to set up sub-committees and working groups of the FGP Committee as required (within the remit of areas of responsibility of the committee) and to set the terms of reference for such groups.
- f) To delegate to the Clerk and other officers, if required, any decision making within its powers to delegate to allow progression of Council business in a timely manner between meetings.

**Note that a Council and its Committees CANNOT delegate any decision making to individual councillors or groups of councillors such as a working party.**

#### **5) Meetings of the Committee**

---

<sup>4</sup> Unlike other committees, this delegation is not restricted to particular budget lines.

Appendix 1 – Draft minutes of the meeting of 14<sup>th</sup> February 2019

- a) The Committee should meet at least six times a year. Agreed dates of meetings should be published in the Council’s Meeting calendar. The Committee should ensure its meetings provide the Council with either a Full Council meeting or an FPG meeting at least every once every calendar month.
- b) The Clerk of the Council will issue a summons and agenda at least three days before each committee meeting. In the event the Clerk is absent and unable to issue the agenda, the agenda and summons will be issued by the chair.
- c) Each Committee Meeting should be attended by the RFO and Clerk to the Council who will act in an advisory role and who will ensure all business transacted falls within the remit and powers of the committee. The Clerk/RFO will produce draft minutes of the meeting. In the absence of the Clerk, the person nominated as temporary RFO will attend.
- d) Minutes will be issued in draft form to the following (in the specified order).
  - i) To the Chair for initial comment.
  - ii) After agreement by the chair, to the committee members for comment.
- e) Minutes will be approved at the next meeting of the committee and each page signed by the chair.
- f) The minutes of all the Committee meetings, whether in draft form or approved, will be presented to the next Full Council Meetings and any recommendations made by the Committee or decisions made that the Clerk feels should be ratified by Full Council will be an agenda item of that meeting to obtain Full Council approval.

Approved at the Full Council Meeting dated:

Minute Reference:

Chair:

Clerk:



Ms S Davies  
Kingsgrove Town Council  
Victoria Hall  
Liverpool Road  
Kingsgrove  
Staffordshire  
ST7 4EL

Direct line +44 (0)191 383 6348  
Email local.councils@mazars.co.uk

13 March 2019

Dear Ms Davies

Completion of the audit for the year ended 31 March 2018

We have completed our audit for the year ended 31 March 2018 and I have pleasure in enclosing the certified Annual Governance and Accountability Return. The External Auditor's Certificate and Report is given in Section 3.

If there are any significant matters arising from the audit, they are summarised in the External Auditor's certificate in Section 3. If we have identified minor scope for improvement we have recorded this on page 2 of this letter. The Council must consider these matters and decide what action is required. In most cases this will be self-evident. In some instances we have referred to further guidance available, in particular, in the publication "*Governance and Accountability for Local Councils – A Practitioners' Guide (England) 2010*". This can be obtained via your NALC or SLCC branch, or downloaded free of charge.

*Action you are required to take*

The Accounts and Audit (England) Regulations 2015 set out what you must do at the conclusion of the audit. In summary, you are required to:

Publish (which must include publication on the authority's website) a statement:

- that the audit has been concluded and that the statement of accounts has been published;
- of the rights of inspection conferred on local government electors by section 25 of the Local Audit and Accountability Act 2014; and
- the address at which, and the hours during which, those rights may be exercised.
- Keep copies of the Annual Governance and Accountability Return for purchase by any person on payment of a reasonable sum.
- Ensure that the Annual Governance and Accountability Return remains available for public access for a period of not less than five years beginning with the date on which the Annual Governance and Accountability Return was first published.

*The Accounts and Audit (England) Regulations 2015 do not specify the period that the 'Notice of conclusion of the audit' needs to be on the council's website but this period must be reasonable.*

Mazars LLP – Salvus House - Aykley Heads - Durham - DH1 5TS  
Tel: +44 (0) 191 383 6300 – Fax: +44 (0) 191 383 6350 – [www.mazars.co.uk](http://www.mazars.co.uk)

Mazars LLP is the UK firm of Mazars, an integrated international advisory and accountancy organisation. Mazars LLP is a limited liability partnership registered in England and Wales with registered number OC300299 and with its registered office at Tower Bridge House, 51 Katharine's Way, London E1W 1DD.

We are registered to carry on audit work in the UK and Ireland by the Institute of Chartered Accountants in England and Wales. Details about our audit registration can be viewed at [www.auditregister.org.uk](http://www.auditregister.org.uk) under reference number C001152661.

VAT number: GB 8066 73



## Section 3 – External Auditor Report and Certificate 2017/18

In respect of

**Kidsgrove Town Council**

### 1 Respective responsibilities of the body and the auditor

This authority is responsible for ensuring that its financial management is adequate and effective and that it has a sound system of internal control. The authority prepares an Annual Governance and Accountability Return in accordance with *Proper Practices* which:

- summarises the accounting records for the year ended 31 March 2018; and
- confirms and provides assurance on those matters that are relevant to our duties and responsibilities as external auditors.

Our responsibility is to review Sections 1 and 2 of the Annual Governance and Accountability Return in accordance with guidance issued by the National Audit Office (NAO) on behalf of the Comptroller and Auditor General (see note below). Our work **does not** constitute an audit carried out in accordance with International Standards on Auditing (UK & Ireland) and **does not** provide the same level of assurance that such an audit would do.

### 2 External auditor report 2017/18

Except for the matters reported below on the basis of our review of Sections 1 and 2 of the Annual Governance and Accountability Return, in our opinion the information in Sections 1 and 2 of the Annual Governance and Accountability Return is in accordance with Proper Practices and no other matters have come to our attention giving cause for concern that relevant legislation and regulatory requirements have not been met.

See separate report

(continue on a separate sheet if required)

Other matters not affecting our opinion which we draw to the attention of the authority:

See separate report

(continue on a separate sheet if required)

### 3 External auditor certificate 2017/18

We certify that we have completed our review of Sections 1 and 2 of the Annual Governance and Accountability Return, and discharged our responsibilities under the Local Audit and Accountability Act 2014, for the year ended 31 March 2018.

\*We do not certify completion because:

Not applicable

External Auditor Name

**Mazars LLP, Durham, DH1 5TS**

External Auditor Signature

*Mazars LLP*

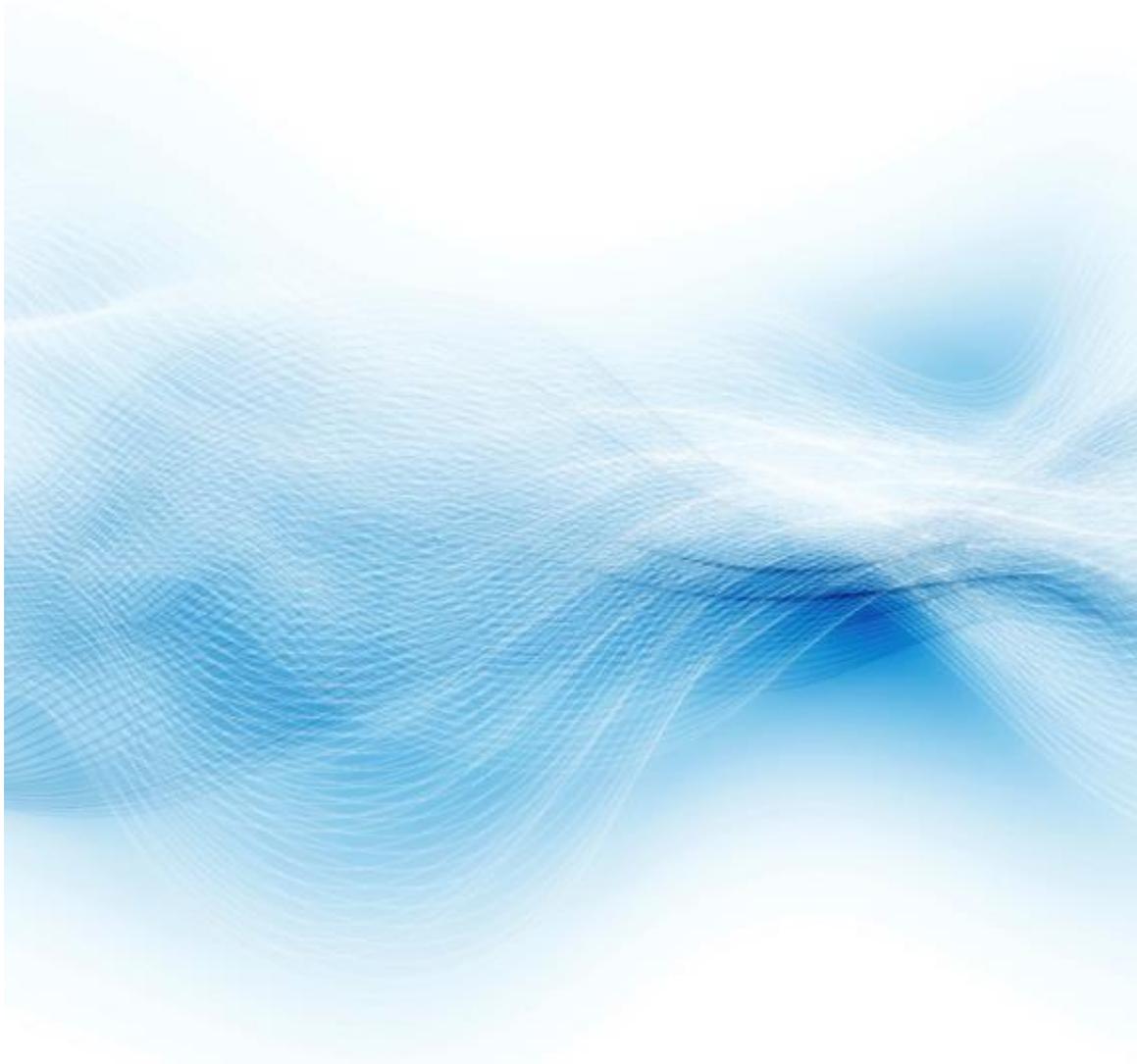
Date

**13 March 2019**

\*Note: the NAO issued guidance applicable to external auditors' work on limited assurance reviews for 2017/18 in Auditor Guidance Note AGN/02. The AGN is available from the NAO website ([www.nao.org.uk](http://www.nao.org.uk))

# External auditor report continuation sheet

Kidsgrove Parish Council  
Year ending 31 March 2018



# 1. INTRODUCTION

## **This page is part of Section 3 – External auditor report 2017/18**

The following matters have been raised to draw items to the attention of Kidsgrove Parish Council. These matters came to the attention of Mazars LLP during the review of the Annual Governance and Accountability Report (AGAR) for the year ended 31 March 2018. This report must be presented alongside the AGAR to a full meeting of the smaller authority for review.

The review of the annual return may not disclose all shortcomings of the systems as some matters may not have come to the attention of the auditor. For this reason, the matters raised may not be the only ones that exist.

**Except for the matters reported below on the basis of our review of the annual return, in our opinion the information in the annual return is in accordance with proper practices and no other matters have come to our attention giving cause for concern that relevant legislative and regulatory requirements have not been met.**

---

The Council has not approved and published the Annual Governance and Accountability Return and started the period of public rights in accordance with the timetable in the Accounts and Audit (England) Regulations 2015. The regulations require these processes to have been completed by the first working day of July. For 2017/18 this was not done until 30 January 2019. For 2018/19 the Council needs to put arrangements in place to ensure that it can discharge its responsibilities in line with the statutory timetable.

The Council has stated in Section 1, item 5, that it has carried out a risk assessment and taken appropriate action to manage those risks including the introduction of internal controls and / or external insurance cover where required. However, Internal Audit reported that the Council did not have sufficient premises and fidelity insurance cover. The Council has taken steps to address this in 2018/19 but should confirm with internal Audit that the revised insurance cover is sufficient.

---

### **Other matters not affecting our opinion which we draw to the attention of the smaller authority:**

During 2017/18 the Council did not meet the requirements of the Accounts and Audit (England) Regulations 2015 in providing electors with a period of 30 working days, including the first 10 working days of July, to inspect the accounts. The Council correctly answered no to the relevant assertion in the 2017/18 Annual Governance Statement and the non-compliance was the unavoidable consequence of the late approval referred to in the qualification above.

The Council has not fully implemented recommendations made in 2016/17 internal and / or external audit reports. In undertaking the review of the 2017/2018 Annual Governance and Accountability Return it came to our attention that in 2018 the Council has again not met the requirements of the 2015 Regulations to provide electors with a period of 30 working days, including the first 10 working days of July, to inspect the accounts. The Council has correctly answered no to the relevant assertions in the 2017/18 Annual Governance Statement. In future, the Council should ensure that appropriate action in response to audit recommendations is taken within a reasonable time. The Council should also answer no to assertion 4 in the 2018/19 Annual Governance Statement.

The 2017/18 internal audit report identified significant weaknesses in internal control. The Council has correctly answered no to assertion 4 in its annual governance statement. The Council should ensure that it implements internal audit recommendations promptly.

---



# GDPR review

Draft Report

Kidsgrove Town Council

John Henry

March 2019

JDH Business Services Ltd

<b>CONTENTS</b>	<b>Page</b>
<b>INTRODUCTION</b>	
<b>WORK DONE</b>	
<b>RESULTS:</b>	
<b>Current Data Subjects and Data Processors</b>	
<b>Current Data Policies</b>	
<b>The General Data Protection Regulation:</b>	
• <b>GDPR Principles</b>	
• <b>Review of current council security arrangements</b>	
• <b>Consent</b>	
• <b>Privacy Notices</b>	
• <b>Data Sharing Agreements</b>	
• <b>Privacy Impact Assessments (PIAs)</b>	
• <b>Notification to the ICO</b>	
• <b>Data Breaches</b>	
• <b>Subject Access Requests (SAR)</b>	
• <b>Data Subject Rights</b>	
<b>CONCLUSIONS</b>	
<b>ACTION PLAN</b>	

Please Note: This report is advisory in nature, informational in content, and is intended to assist the council to improve their standards of compliance with data protection legislation and best practice; it does not constitute legal advice. It has been based on observations and written and oral information provided by the council's representative(s). This report, however, has been prepared on the strict understanding that the council retains ownership of, and remains responsible for, the compliance with data protection in its workplace. Accordingly, JDH Business Services Ltd will not accept liability for any incident or damages of any kind resulting from the use of, or reliance upon, any information contained in the report.

## **Introduction**

The new General Data Protection Regulation (GDPR) became enforceable from May 25<sup>th</sup> 2018, and the UK Data Protection Act 2018 will become law in 2018. GDPR will increase individuals' rights on personal data and will therefore significantly tighten up the rules on privacy and consent. Councils will need to identify their lawful basis for processing personal data and demonstrate compliance with the GDPR principles. Decision makers and key people in the council will need to appreciate the impact of GDPR including subject access request procedures and data breach procedures to detect, report and investigate a personal data breach. Councils will also need to ensure data protection is by design and utilise Privacy Impact Assessments when required.

The GDPR aims to achieve an improvement in the balance between the requirements of organisations that collect and process personal data (ie the data controllers and data processors) and the rights that data subjects have to privacy and to have their personal and sensitive data kept secure, whether as manual or electronic data. Therefore, the GDPR will increase the rights of data subjects and increase the obligations of data controllers and data processors. The council is both a data controller and a data processor.

The council is responsible for compliance with the GDPR and data protection law and not the Data Protection Officer (DPO) whose role is to independently assess compliance on an ongoing basis. The council should exercise proper control and management of personal data as this will be fundamental to ensuring, and demonstrating, compliance with the GDPR. Transitioning to the new regime may be challenging and to support the transition, as part of our role as the DPO, we have completed a review to assess readiness for the GDPR.

## **Work Done**

Current data subject categories and third parties who process data for the council were identified through discussion with staff. Information was compiled to enable a draft data inventory of the personal data that is processed by the council to be completed detailing whose personal data is processed, the purpose, type, source, lawful basis, location, frequency, retention period, legal determination of retention, and security arrangements for data protection.

A data protection review was carried out to evaluate current personal data processing controls and procedures against the GDPR requirements to identify new or improved internal controls, procedures, accountability and risk-based security actions to be implemented. The review also included the following:

- Assessment of all data policies
- Assessment of current security arrangements for electronic and manual personal data records

## **Current Data Subjects and Data Processors**

Data subjects are identified, or identifiable natural living persons and we identified through discussion with council officers that the council processes personal data for the following categories of data subject:

- Employees
- Members - bank authorisation personal data used for online banking
- Consultees – future consultations are planned using Survey monkey and manual exercises
- Complainants and enquirers about the council’s own services, and enquiries about other third-party services eg.) unitary authority services
- Grants and donations - financial assistance applications where an individual’s personal contact details are included.
- Photographed individuals at events by members and staff
- Ranger services - photographs are currently the only personal data collected by this service
- Third party emails and contacts details eg individuals, businesses, public sector, voluntary sector, that can be identified with a data subject
- Competition entrants
- Room hire booking forms
- Newsletter registration via the website
- Directly managed allotments
- Volunteers at events eg Party in the Park
- Ticket sales - name and address retained to provide receipt and inform of cancellations

### ***Recommendation***

***The document retention policy should be updated to reflect the data subject categories listed above and set time limits for their personal data retention.***

A data processor means a legal person, public authority, agency or other body which processes personal data on behalf of the data controller. The council is the data controller and as some of the other data subject categories listed above are processed internally, the council is also an internal data processor. We were informed that the external (third-party) data processors are:

- Statutory bodies including HMRC
- The pensions administrator Staffordshire Pension Fund
- The payroll agent
- The health and safety adviser Ellis Whitham
- The website host and email provider
- The IT provider

## **Current Data Policies**

---

It was not clear if the council has adopted the comprehensive data protection policy on file and this is not published in the council website. A communication and social media policy has not been adopted. There is no information security policy in place.

***The council should adopt the following:***

- ***the GDPR compliant data protection policy***
- ***an information security policy which also identifies security requirements for members.***
- ***a communication and social media policy.***

A document retention policy has not been adopted. This key policy will provide the council with a simple framework as to how long documents of different categories should be retained, when they should be disposed of and secure disposal requirements. The policy will also help the council save time and storage space by reducing the amount of information held unnecessarily. Apart from providing a framework as to how long documents of different categories should be retained, the policy will be essential for evidencing compliance with aspects of the GDPR principles described above. As previously noted, the retention policy will need to cover all the data subject categories listed above and therefore how long their records will be retained.

***The council should adopt a document retention policy and adhere strictly to the retention deadlines in the document retention policy. In particular, the council should ensure it is not retaining personal data longer than is necessary to complete the specified purpose(s).***

***There will need to be time allocated to permanently delete and shred legacy personal data, and other information held in excess of the time limits set in the newly adopted retention of documents policy.***

## **The General Data Protection Regulation**

### **GDPR Principles**

The GDPR consolidates the eight principles of the Data Protection Act 1998 into six principles:

- Personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject (ie a living individual)
- All personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes
- The personal data collected and retained must be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed
- All personal data collected must be accurate and, where necessary, kept up to date

- The personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data are processed
- Personal data must be processed in a manner that ensure appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

**Impact on the council:**

*The council have already incorporated the above six GDPR principles in the new data protection policy which now needs to be adopted at full council.*

**Review of current council security arrangements:**

	<b>Current procedures</b>	<b>Improvements</b>
Email	All officers and members have unique email addresses through exchange, however, there are issues with these email accounts so to be sure all members receive information the emails are also forwarded to member private email accounts. There is also a current problem with applying searches to council hosted email accounts,	<p><i>The email host organisation should be asked to urgently resolve the issues being encountered with the council email accounts. Members should use town council email addresses for town council business.</i></p> <p><i>When a member ceases to be a member, the limits set in the retention policy should be applied to the email history of the councilor. This may be difficult to apply if a non-council email address is used by a member.</i></p> <p><i>Security procedures for members should be included in the information security policy</i></p>
Passwords	All staff have separate logins. There are no automatic prompts to change passwords.	<i>The IT provider should be asked to set up automatic prompts for password changes at a frequency to be determined by the councils.</i>

	<b>Current procedures</b>	<b>Improvements</b>
		<i>Secure password best practice should be followed</i>
Document Security	<p>The document archive comprises two locations:</p> <ol style="list-style-type: none"> <li>1. A locked room in the council building to which the clerk, assistant and security contractor have access. The files in this room are stored on shelves or unlocked cabinets.</li> <li>2. An offsite archive in a joiners yard currently costing £80 a month. The clerk and a member are going to visit this site to determine the quantities and types of information stored there. The provider has a key to this offsite storage.</li> </ol> <p>There is no public reception and the public cannot access the council offices unsupervised.</p> <p>The Security contractor has keys to the council offices and also take photocopies of the diaries.</p>	<p><i>Cabinets containing personal information should be locked.</i></p> <p><i>The council should consider moving the archive storage from the Joiners Yard to the archive room in the council building.</i></p> <p><i>All archived personal information held in excess of the retention deadlines in the document retention policy should be securely shredded.</i></p> <p><i>The security contractor should return all copies of diaries to the clerk when they are finished with.</i></p>
Desktop Computers	<p>Two desktops are used in the council offices. No obsolete computers are retained at the premises.</p> <p>Up to date antivirus software is installed and the computer screens are locked down when not in use - automatic updates have been installed. A firewall has been installed.</p> <p>Cloud based back up is provided via Dropbox.</p>	<p><i>The council should discuss with the IT provider the most effective anti-virus software and firewall for the council requirements and ensure it is updated regularly to cover the latest identified cybersecurity threats.</i></p> <p><i>To counteract phishing attacks, the council</i></p>

	<b>Current procedures</b>	<b>Improvements</b>
	<p>Permanent file deletion software is not installed.</p> <p>Payroll is emailed without encryption. An email document encryption facility is not utilised to send payroll information to the payroll agent.</p>	<p><i>should check with the IT provider whether an appropriate multi-layered approach is in place using two-factor authentication, email filters and anti-spoofing controls. In addition there should be raised awareness amongst staff and members via training on the identification of malicious content.</i></p> <p><i>Permanent file deletion software should be installed and utilised.</i></p> <p><i>The council should ensure email encryption is available when required for emailing sensitive personal data such as payroll information.</i></p> <p><i>Personal information stored on the computer drives should be reviewed by reference to the newly adopted retention policy and data no longer required should be permanently deleted.</i></p>
Photographs	<p>Photographs are taken at events by members or staff and by the ranger.</p> <p>Signage that communicates to the public that photos are being taken is not used.</p>	<p><i>Photographs should be securely stored until destruction or permanent deletion with all other personal data types. Photographs still held on private mobile phones that relate to council business should be erased in accordance with the council retention policy.</i></p> <p><i>Appropriate signage should be displayed at all events and GDPR compliant image consent</i></p>

	<b>Current procedures</b>	<b>Improvements</b>
		<p><i>forms should be used where required</i></p> <p><i>Photographs should be included in the retention policy</i></p>

## Consent

Data controllers must have a legitimate reason(s) for collecting and processing personal data and if the data controller is relying on a data subject's consent they have to be able to evidence that consent; by a statement or by a clear affirmative action, that consent was freely given, specific, informed and unambiguous for each purpose that it is being processed. Prior to giving consent, the data subject should be informed of their right to withdraw consent at any time. Therefore, it should always be as easy to withdraw consent as to give consent. There are also changes further consent requirements under the GDPR but the council has confirmed it does not collect and process any children's personal data.

There are alternatives to consent as a lawful basis for processing personal data. These are set out in Article 6(1) of the GDPR. In summary, the council can process personal data without consent if it is necessary for:

- A contract with the individual: for example, to supply goods or services they have requested, or to fulfil obligations under an employment contract. This also includes steps taken at their request before entering into a contract.
- Compliance with a legal obligation: if the council is required by UK or EU law to process the data for a particular purpose
- Vital interests: the council can process personal data if it is necessary to protect someone's life. This could be the life of the data subject or someone else. For instance, a council collects emergency contacts for employees in case of an emergency.
- A public task: if a council needs to process personal data to carry out official functions or a task in the public interest, and the council has a legal basis for the processing under UK law. **Therefore, as a UK public authority, the ICO view is that this is likely to give the council a lawful basis for many of your activities.**
- Legitimate interests: a private-sector organisation, can process personal data without consent if it has a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests. Public bodies such as councils cannot generally rely on 'legitimate interests' under the

GDPR but should consider the ‘public task’ basis instead, although there are occasions when legitimate interests can be used as a lawful basis by public bodies.

The public task basis for processing:

The public task basis in Article 6(1)(e) of the GDPR may appear new, but it is similar to the old condition for processing for functions of a public nature in Schedule 2 of the Data Protection Act 1998. A council can rely on this lawful basis if it needs to process personal data:

- ‘in the exercise of official authority’. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.

The council does not need a specific statutory power to process personal data, but the underlying task, function or power must have a clear basis in law. If the council can demonstrate it is exercising official authority, including use of discretionary powers, there is no additional public interest test. However, the council must be able to demonstrate that the processing is ‘necessary’ for that purpose. If the council could reasonably perform the task or exercise powers in a less intrusive way, this lawful basis does not apply. The council should document the decision to rely on this basis to help demonstrate compliance. The council should be able to specify the relevant task, function or power, and identify its statutory or common law basis. The council must also update the relevant privacy notice to include the lawful basis and communicate this to individuals.

Individuals’ rights to erasure and data portability are more limited if the council is processing on the basis of public task. However, individuals do have a right to object. The council should consider an alternative lawful basis if it is not confident that processing is necessary for a relevant task, function or power which is clearly set out in law.

**Impact on the council:**

The council processes employee personal data and this is covered by the employment contract lawful basis.

The council does not need consent for any of the other following service activities which process personal data as they are all covered by the Public Task lawful basis:

- Members bank authorisation data for members for online banking
- Consultees
- Complainants and enquirers about the council’s own services
- Grants and donations - financial assistance applications where an individual’s personal contact details are included.

- Third party emails and contacts details eg individuals, businesses, public sector, voluntary sector, that can be identified with a data subject
- Competition entrants
- Room hirers
- Newsletter registration via the website
- Directly managed allotments
- Volunteers at events eg Party in the Park
- Ticket sales

***Consent will be needed for the following:***

- ***Enquiries received by letter, email or telephone which relate to third party services eg police, housing associations and the council needs to forward personal details to a third party***
- ***Photographed individuals at events and by the ranger.*** The ranger is seconded from the borough council. The consent form used at schools now includes website, social media and publications. Any photos at schools require a teacher or supervisor to sign the consent form to confirm that parental permissions have been granted. This form is currently only sent to the borough council but needs to also be sent to the town council as evidence. For other events such as the litter pick with Kidsgrove care solutions and Coop members, a consent form is not currently used so the practice of using image consent forms for all organisations should be introduced for this service.

***Appropriate signage should be used at events so people are fully informed that photos are being taken and are able to opt out if they wish.***

***The schools consent form should be sent to the town council as evidence consent was obtained whilst acting on behalf of the town council.***

***A GDPR compliant consent form should be used when taking images of individuals from other organisations participating in litter picks.***

***If any photographs are taken of minors that, along with other information, can be identified with an individual then the use of these images of minors without guardian consent is a non-compliance under GDPR so clearly appropriate consent is mandatory. The council should identify scenarios where images may be used and set out clear guidelines to ensure processing is lawful in such situations.***

***An example approach for non-minor images may be to state within an information security policy that non-identifiable images e.g. group photographs or background photographs, may be used without prior consent (although signage informs people at events that they can opt out). But that any image, when used with associated information, that can uniquely identify an individual, requires written consent before it can be published externally, including on the council website. Once consent has been obtained, the council must ensure they protect the confidentiality of the images until they are permanently deleted in accordance with the retention policy.***

## **Privacy Notices**

The GDPR requires more detailed information to be provided by data controllers in privacy notices:

- The identity and contact details of the data controller and, if any, the controller's representative and the data protection officer
- The purpose(s) of the personal data processing
- The categories of personal data required
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular, recipients in third countries or international organisations
- Where possible, the envisaged period for which the personal information will be stored, or, if not possible, the criteria used to determine that period
- The right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint to the ICO
- Where the personal information is not collected from the data subject, any information as to its source

Information included in a privacy notice, or any communication to the data subject about their rights, must be concise and intelligible using clear and plain language, suitable to the age of data subject being communicated with. The information must be provided in writing, or by other means, including where appropriate electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. Therefore, the council will need to establish a robust identification procedure to verify the data subject.

### **Impact on the council:**

The categories of privacy notice required for the council are:

- Employees, volunteers and any councilors whose payroll details are held
- All Service Users and residents, including complainants and enquirers, and third parties

The council has not published an external privacy notice for all service users and residents on the website. There is no internal privacy policy for employees/members/volunteers.

***The council should adopt and publish GDPR compliant internal and external privacy notices***

## **Data Sharing/Processing Agreements**

The council as a data controller must enter into a contract with every third-party data processor which imposes the following stipulations on the data processor:

- Personal data can only be processed based on the scope of the documented instructions of the data controller. This will mean that data processors cannot use cloud computing technology or services without the data controller's approval
- Compliance with security obligations equivalent to those imposed on the data controller by the GDPR (Article 32)
- Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality
- Enlist a sub-processor only with the prior permission of the data controller
- Assist the data controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR
- Assist the data controller in carrying out its data security obligations under the GDPR

**Impact on the council:**

The council confirmed that the current external non-statutory data processors or third parties with access to council information are:

- The payroll agent
- The health and safety adviser Ellis Whitham
- Website host and email provider
- IT provider

None of the above has signed a data processing/sharing agreement

*Where the council determines that it is sharing data with relevant third parties and/or third parties are processing council personal data, a signed data sharing/processing agreement needs to be implemented, and where encryption is required (eg for payroll information) the council should ensure the external provider has implemented this.*

**Privacy Impact Assessments (PIAs)**

This is a process which assists in identifying and minimising privacy risks to data subjects of new services or projects and involves working with people who may be affected to identify and reduce privacy risks. The aim of conducting PIAs is to ensure potential problems and high risks are identified at an early stage of a new service or project and that privacy is by design individuals.

**Impact on the council:**

Currently the council is not directly delivering services or projects that would require a PIA to be carried out.

*The council should adopt a PIA process that utilises a best practice template which will enable a PIA to be carried out effectively where required in the future.*

### **Notification to the ICO**

This requirement under the Data Protection Act 1998 is to be replaced by a new requirement for data controllers to maintain a written record of processing activities under their responsibility. The record shall include a description of the categories of data subjects and the categories of personal data, purpose(s) of processing, categories of recipients of personal data, time limits for erasure and description of organisational and technical measures to protect the data. Data processors also have a new duty to maintain a record of similar information. However, the requirement to maintain a written record does not apply to an organisation employing less than 250 persons unless the processing results in risks to the rights of data subjects, the processing is not occasional, or the processing includes sensitive personal data.

#### **Impact on the council:**

In practice it would be very difficult for the council to evidence full compliance with the GDPR principles and requirements if it did not have an up to date personal data inventory. The personal data inventory should identify for every category of data the lawful basis for collecting, processing and storing the personal data.

*The council should compile a complete data inventory to evidence compliance with the GDPR and the new rights of data subjects. We have supported the clerk with compiling the data inventory for all personal data held.*

### **Data Breaches**

The council as data controller only has to notify the ICO where a data breach is likely to result in a risk to the rights and freedoms of the individuals affected. For example, if the data breach could lead to discrimination, financial loss, reputational damage, loss of confidentiality or any other significant economic or social disadvantage. Therefore, the council as a data controller should have appropriate procedures in place to detect, report and investigate a personal data breach. Data controllers will be required to report to the ICO without delay and definitely within 72 hours, any identified personal data breaches. In some cases data breaches will need to be reported to the data subjects where the breach is likely to result in a high risk to the rights and freedoms of individuals.

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

#### **Impact on the council:**

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

*We have provided the GDPR requirements for data breaches to the council and these are included in the Data Protection procedures published by the council. Staff should ensure the requirement for data breaches under the GDPR are understood.*

### **Subject Access Requests (SAR)**

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

- In the majority of cases the council will not be able to charge a fee for complying with a SAR, which is a right of access to the individual's personal data held by the council as data controller
- The council will have 1 month to comply with a SAR (up to May 25<sup>th</sup>, 2018 the deadline is 40 days)
- The council can charge a fee for requests that are manifestly unfounded or excessive or repetitive and can refuse to respond
- If the council refuses a request, the individual must be told why and informed of their right to complain to the ICO and to a judicial remedy. The individual must be informed of the decision without undue delay and at the latest within 1 month.

### **Impact on the council:**

*We have provided the GDPR requirements for Subject Access Requests to the council. These procedures should be clearly understood by council staff. Template letters should be in place to deal with key stages of an SAR including securing third party input where required.*

### **Data Subject Rights**

In addition to being able to submit SARs described above data subjects have the rights to:

- restrict processing of their personal data
- new limited rights against data processors
- object to processing of their personal data for direct marketing purposes
- not be subject to automated decision-making
- receive compensation from the data controller AND the data processor for the damage suffered as a result of an infringement of the GDPR
- obtain from a data controller without undue delay the rectification of inaccurate personal data
- ask the data controller to erase their personal data and to no longer process it (the right to be forgotten). This could be where the data is no longer necessary in relation to the purpose for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the GDPR. However, further retention of the personal data will be lawful in certain circumstances. For councils, an example is where the data is required for compliance with a legal obligation. Where the data controller has made the personal

data public and is obliged to erase the personal data it shall take reasonable steps to inform data controllers and processors who are processing the personal data that the data subject has requested them to erase any links to, or copy or replication of that personal data

- be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights
- data portability ie to receive a copy of personal data or to transfer personal data to another data controller

**Impact on the council:**

*The Data Protection policy and privacy notices that are to be adopted should include the rights of data subjects as prescribed by the GDPR. The council staff will need to understand the new data subject rights under the GDPR.*

**Training**

*Data Protection and cybersecurity training should be provided at induction to employees and members, and on an ongoing basis.*

**Conclusions**

There are a number of areas where the council needs to take action to help ensure compliance with data protection good practice and the GDPR:

- adopting key policies including data protection, information security, communications and social media, and a retention policy for all categories of data subject
- adopting and publishing GDPR compliant external and internal privacy notices
- improving manual and electronic document security arrangements as recommended
- completing the council data inventory on an ongoing basis, including the correct lawful bases for holding personal data
- ensuring personal information is only retained for as long as required for the purposes of processing and according to statutory requirements. This will require ongoing compliance with the adopted retention policy
- implementing data sharing/processing agreements where personal data is shared/processed by third parties
- ensuring valid consents are obtained where consent is the lawful basis for retaining personal data

- adopting a Privacy Impact Assessment (PIA) process
- ensuring ongoing data protection and GDPR awareness training of staff and members

The action plan overleaf includes the detailed recommendations arising from the review to help address the above issues. The action plan prioritises issues as ‘Fundamental’, ‘Significant’ and ‘Merits Attention’.

### ACTION PLAN

The priority of the recommendations made is as follows:

Fundamental	Significant	Merits Attention
Action is required to ensure that the GDPR is met	Action is required to avoid exposure to significant risk in achieving the GDPR	Action is advised to enhance personal data controls and security

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<i>The council should adopt and publish a GDPR compliant data protection policy</i>	Fundamental				
	<i>The council should compile a data inventory to evidence compliance with the GDPR, in particular:</i> - <i>the correct lawful basis should be identified for retaining personal data</i>	Fundamental		NB We have assisted the council with completion of a draft data inventory.		

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<ul style="list-style-type: none"> <li>- <i>all data subject categories as specified in this report should be included</i></li> <li>- <i>whether or not a data breach should be reported to the ICO for each data subject personal information category if there was a breach</i></li> </ul>					
	<p><i>The council should adopt an information security policy which also identifies security requirements for members.</i></p>	Significant				
	<p><i>The council should adopt a communication and social media policy.</i></p>	Significant				
	<p><i>A document retention policy should be adopted. The retention policy should include the data subject categories listed in this report and set time limits for their personal data retention.</i></p> <p><i>There will need to be time allocated to permanently delete and shred legacy personal data, and other</i></p>	Fundamental				

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<i>information held in excess of the time limits set in the newly adopted retention of documents policy.</i>					
	<i>The email host organisation should be asked to urgently resolve the issues being encountered with the council email accounts. Members should use town council email addresses for town council business.</i>	Significant				
	<p><i>Manual Document Security issues:</i></p> <p><i>Cabinets containing personal information should be locked.</i></p> <p><i>The council should consider moving the archive storage from the Joiners Yard to the archive room in the council building.</i></p> <p><i>The security contractor should return all copies of diaries to the clerk when they are finished with.</i></p>	Significant				
	<i>Permanent file deletion software should be installed and utilised.</i>	Fundamental				

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<i>Data Protection and cybersecurity training should be provided at induction to employees and members, and on an ongoing basis.</i>	Fundamental				
	<i>All archived personal information held in excess of the retention deadlines in the document retention policy should be securely shredded</i>  <i>Personal information stored on the computer drives should be reviewed by reference to the newly adopted retention policy and data no longer required should be permanently deleted.</i>	Fundamental				
	<i>The IT provider should be asked to set up automatic prompts for password changes at a frequency to be determined by the councils.</i>  <i>Secure password best practice should be followed</i>	Merits Attention				
	<i>The council should discuss with the IT provider the most effective anti-virus software and firewall for the council requirements and ensure it is</i>	Fundamental				

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<p><i>updated regularly to cover the latest identified cybersecurity threats.</i></p> <p><i>To counteract phishing attacks, the council should check with the IT provider whether an appropriate multi-layered approach is in place using two-factor authentication, email filters and anti-spoofing controls. In addition there should be raised awareness amongst staff and members via training on the identification of malicious content.</i></p>					
	<p><i>The council should ensure email encryption is available when required for emailing sensitive personal data.</i></p>	<p>Significant</p>				
	<p><i>Photographs should be securely stored until destruction or permanent deletion with all other personal data types. Photographs still held on private mobile phones that relate to council business should be erased in accordance with the council retention policy.</i></p>	<p>Fundamental</p>				

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<p><i>Photographs should be included in the retention policy as a personal data category</i></p> <p><i>Appropriate signage must be displayed at all events and GDPR compliant image consent forms should be used where required</i></p>					
	<p><i>Ranger Services - Photographs:</i></p> <p><i>The schools consent form should be sent to the town council as evidence consent was obtained whilst acting on behalf of the town council.</i></p> <p><i>A GDPR compliant consent form should be used when taking images of individuals from other organisations participating in litter picks.</i></p>	<p>Fundamental</p>				
	<p><i>Appropriate consent will need to be secured (and retained) for the following:</i></p> <ul style="list-style-type: none"> <li><i>Enquiries received by letter, email or telephone which relate to third party services eg housing associations, unitary authority and the council needs to forward personal details to</i></li> </ul>	<p>Fundamental</p>				

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<p><i>a third party</i></p> <ul style="list-style-type: none"> <li><i>Photographs are taken at certain events and by the ranger and may be published in a wide variety of council media.</i></li> </ul> <p><i>If any photographs are taken of minors that, along with other information, can be identified with an individual then the use of these images of minors without guardian consent is a non-compliance under GDPR so clearly appropriate consent is mandatory. The council should identify scenarios where images may be used and set out clear guidelines to ensure processing is lawful in such situations.</i></p> <p><i>An example approach for non-minor images may be to state within an information security policy that non-identifiable images e.g. group photographs or background photographs, may be used without prior consent (although signage informs people at events that they can opt out). But that any image, when used with associated information, that can uniquely identify an</i></p>					

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<i>individual, requires written consent before it can be published externally, including on the council website. Once consent has been obtained, the council must ensure they protect the confidentiality of the images until they are permanently deleted in accordance with the retention policy.</i>					
	<i>The council should adopt and publish GDPR compliant internal and external privacy notices</i>	Fundamental				
	<i>Where the council determines that it is sharing data with relevant third parties and/or third parties are processing council personal data, a signed data sharing/processing agreement needs to be implemented, and where encryption is required the council should ensure the external provider has implemented this.</i>	Fundamental				
	<i>The GDPR requirements for Data Breaches and Subject Access Requests should be clearly understood by council staff. Robust template letters should be in place to deal with all key stages of an SAR including securing third party exemption where required.</i>	Fundamental				

Appendix 3 – Draft GDPR Report

Ref	Recommendation	Categorisation	Accepted (Y/N)	Council Comment	Implementation Date	Responsibility
	<p><i>The council should adopt a Privacy Impact Assessment process that utilises a best practice template which will enable a PIA to be carried out effectively where required in the future.</i></p>	<p>Significant</p>				

## Bar Contract Task Group

Kidsgrove Town Council  
Victoria Hall  
Liverpool Road  
Kidsgrove  
Staffordshire  
ST7 4EL

Tel: 01782 782254

[www.kidsgrovetowncouncil.gov.uk](http://www.kidsgrovetowncouncil.gov.uk)



### Terms of Reference

#### General

1. The task group to be set up under and reporting into the F&GP Committee.
2. The task group to be strictly advisory with no delegated decision-making powers.
3. The task group to consist of at least six members with a chair elected at the first meeting.
4. The task group to be attended by the Clerk who will produce agendas and minutes.
5. Due to commercial sensitivity, that the contents of the minutes of the meeting are considered strictly confidential to be reported to F&GP under Part 2 (press and public excluded).
6. That any tendering process strictly follows the Council's financial regulations and any other legislation applicable.

#### Purpose and Aims

That the Task Group consider and evaluate the future of the Victoria Hall Tap Room and make recommendations to the F&GP Committee. The consideration will include the future management, potential contracts, earning capacity versus costs to the council, opening hours and the role of the bar during commercial and community events.