nalc
National Association
of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk

w: www.nalc.gov.uk
a: 109 Great Russell Street,
London WC1B 3LD

NATIONAL ASSEMBLY | AGENDA

Date and time: 9 March 2021, 11:00 – 13:00.

Introductions and welcome – 10:45 – 11:00

Via zoom.

1. **Welcome by the Chairman**

2. **Apologies for absence and note changes in representation**

   2.1. That apologies are noted.

   2.2. That new representatives introduce themselves to National Assembly.

   - Cllr Brian Brooks, East Riding North Lincolnshire of Local Councils
   - Cllr Alan Humphries, Worcestershire Association of Local Councils
   - Cllr Janet Wallace, Dorset Association of Local Councils
   - Cllr Jenny Lawrence, Somerset Association of Local Councils
   - Cllr Dave Fleming, County Durham Association of Local Councils
   - Cllr Malcolm Butler, Hampshire Association of Local Councils
   - Cllr Jonathan Davies, Cumbria Association of Local Councils

3. **Minutes of previous meeting**

   3.1. To approve the minutes of the National Assembly held on 8 December 2020 and to consider any matters arising. Appendix 3.1

4. **Committee Issues (11:15 – 11:30)**

   4.1. To receive summary highlight reports from committee chairs. Appendix 4.1

5. **Civility in the sector: NALC position on the LGA's national code of conduct. Joint work with Society of Local Council Clerks (SLCC) (11:30 – 12:00)** Appendix 5.1

Tea break – 12:00 -12:15

6. Launch of Good Councillors Guide to Cyber Security in partnership with Micro shade (12:15 – 12:30)

6.1. David Astwood from Microshade will be joining the meeting to provide an update. (attached paper)

7. Task and Finish Group – Governance (12:30 – 12:45)

7.1. To discuss the recent meetings of the Task and Finish Group on Governance. Minutes of recent meetings attached.

8. Monitoring and managing performance and service delivery (12:45 – 13:00)

8.1. To note the latest corporate performance statistics and NALC activity report. Appendix 8.1.

9. Next meeting

That the next meeting of National Assembly be held on 13 July 2021 via zoom. We are also proposing to hold more open councillor sessions in the April and June. Dates to be confirmed.

nalc
National Association
of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk

w: www.nalc.gov.uk
a: 109 Great Russell Street,
London WC1B 3LD

NATIONAL ASSEMBLY | DRAFT MINUTES

8 December 2020

Via zoom

National Assembly	
Cllr Mike Drew	Avon Association of Local Councils
Cllr Elizabeth Luder	Bedfordshire Association of Town and Parish Councils
Cllr Mike Tew	Cambridgeshire Association of Local Councils
Cllr Lillian Burns	Cheshire Association of Local Councils
Cllr Graham Ford	Cornwall Association of Local Councils
Cllr John Plant	Derbyshire Association of Local Councils
Cllr Ken Browse	Devon Association of Local Councils
Cllr Janet Wallace	Dorset Association of Parish and Town Councils
Cllr Keith Stevens	East Sussex Association of Local Councils
Cllr Peter Davey	Essex Association of Local Councils
Cllr Loraine Rappé	Hampshire Association of Local Councils
Cllr Rob McCarthy	Hertfordshire Association of Local Councils
Cllr Bob Blezzard	Isle of Wight Association of Local Councils
Cllr Richard Parry	Kent Association of Local Councils
Cllr Colin Peacock	Lancashire Association of Local Councils
Cllr Tony Howard	Lincolnshire Association of Local Councils
Cllr Tony Hirons	Leichestershire and Rutland Association of Local Councils

Cllr Phil Harris	Norfolk Association of Local Councils
Cllr Mick Baker	Nottinghamshire Association of Local Councils
Cllr David Francis	Northumberland Association of Local Councils
Cllr Malcolm Leeding MBE	Oxfordshire Association Local Councils
Cllr David Beechey	Shropshire Association of Local Councils
Cllr Steve Cosser	Surrey Association of Local Councils
Cllr Loretta Whetlor	Somerset Association Local Councils
Cllr Mark Valladares	Suffolk Association of Local Councils
Cllr Rosie Weaver, BEM (for part)	Warwickshire and West Midlands Association of Local Councils
Cllr Peter Allison	West Yorkshire Association of Local Councils
Cllr Terry Oliver	West Sussex Association of Local Councils
Cllr John Scragg	Wiltshire Association of Local Councils
Cllr Brian Kerr, OBE	Vice president

Staff present:
Jonathan Owen, chief executive
Justin Griggs, head of policy & communications
Charlotte Eisenhart, head of member services
Steve Walker, head of finance and administration
Claire Goldfinch, projects officer (for part)
Farhana Miah, executive officer
Olivia Cane, receptionist
Claire Fitzgerald, administration manager
Linda Hammond, projects officer.

<u>Chairman welcome:</u>

The chairman welcomed representatives to the meeting and asked assembly members to reflect on the following colleagues who had recently passed away:

- Cllr Ken Cleary (former NALC chairman)
- Cllr Gordon Thurston

Minutes of the previous meeting:

The Assembly confirmed that the minutes of the meeting of National Assembly held on 14 July were accurate. Minutes of the open councillor sessions in August and September were also noted.

In matters arising Cllr Parry queried if NALC had any update on the work conducted with Secretary of State Robert Jenrick MP on funding. The chairman assured Cllr Parry that strong representations had been made and the issue had been raised in the House of Lords too it was mentioned in the House of Lords, and will be continued in NALC's lobbying activity.

RESOLVED: That the chairman be authorised to sign the draft minutes of National Assembly held on 14 July 2020 as a true record of the proceedings.

Changes in representation:

The following changes in representation were noted:

- Cllr Mark Valladares, Suffolk Association of Local Councils
- Cllr Steve Cosser, Surrey Association of Local Councils
- Cllr Phil Harris, Norfolk Association of Local Councils
- Cllr Janet Wallace, Dorset Association of Local Councils

The new councillors were welcomed and each briefly introduced themselves setting out their experience and ambitions fir the sector

NALC committee elections:

The chief executive updated the Assembly that Due to a technical glitch the elections to the vacancies on the smaller councils committee and finance and scrutiny committee had been adversely affected. The chief executive had briefed the chairman and vice-chairmen on this and it was concluded that there is no alternative to re-running the process. The elections will be conducted again by an online ballot to include all candidates who submitted their nominations within the timescales. In addition to this the elections process will be reviewed in light of this ensuring this does not happen again. Chief executive announced that six nominations were had been received:

- Cllr Loretta Whetlor
- Cllr Mark Valladares
- Cllr Bob Blezzard
- Cllr Mike Tew
- Cllr Tony Howard
- Cllr Mike Scott

Cllr Peacock asked if methods of communications could be looked into and chief executive assured this is something that will look into as part of the work of the TWG

NALC governance:

The chairman reported that management board had agreed to establish an Assembly task and finish group to assess the mid to long-term implications of the pandemic for NALC's governance including pro's and con's of continuing with remote meetings and greater use of informal networks. It would also pick up the point raised earlier about communications, availability off core corporate documents and circulation of papers etc.

Cllr Scott noted that the assembly had previously agreed to conduct a review of the the effectiveness of governance arrangements to assess if the objectives had been met and the work of the TWG could feed into this.

Cllr Stevens noted that the finance and scrutiny committee had oversight of the association's wider governance including finance regulations and risk.

The chairman concluded that the finance and scrutiny committee would oversee the general review of the effectiveness of changes in governance and the task and finish group will identify lessons from the pandemic experience. Management board had overall responsibility for recommending any changes to Assembly.

Monitoring and managing performance and service delivery

The chairman asked the assembly if they have any questions on the activity report. Insert link

Cllr Blezzard asked about if there have been any further developments on relations with SLCC and progress on the devolution agenda.

The chairman informed that the devolution paper had been delayed until the summer, although some aspects of local government re-organisation might be addressed separately.

The chief executive reported on a productive meeting with the SLCC including the general issue around civility in public life and relationships between clerks and councillors. There was a broad agreement that this issue would need to be addressed jointly The intention is to have a leadership meeting with NALC chairs and vice-chairs and SLCC colleagues.

Resolved: That the activity report be received.

Good practice session:

Justin Griggs, head of policy and communications introduced discussion of how to take forward the assoiciation's campaign around youth engagement. This would build on the successful approach taken for the health and wellbeing and climate change campaigns, including a:

- Dedicated webpage
- Case studies publication
- NALC event/s
- Articles and media coverage

He welcomed the assembly sharing ideas on what work has been done in their own patch.

Cllr Drew informed that Yate Town Council have regularly meetings with youth council and general consultation. Yate Town Council have extended their work on engaging with youth via a dedicated facility providing different services such as hot drinks, computer usage and engaging with young people about any concerns or interest they may have.

Cllr Parry spoke on how Sevenoaks Town Council had been involved in youth provision and set up a Youth Town Council which had been a success. The town council also have a youth café open and provides different services such as counselling. During the pandemic, in order to engage with youth, the council have set up zoom meetings for young people and summer social distance music events. In addition to this they had set up theatre groups for young people who had an interest in arts.

Cllr Weaver informed that WALC had set up training for all parish and town councils working with youth community. The county association had talked about the importance of social media in order to have engage with the youth more effectively.

Other examples of local initiatives were identified in the zoom chat (attached)

Resolved: That the report be received.

<u>The Good Councillors' Guide to Community Business:</u>

National Assembly members were given a presentation by Chris Cowcher, head of community business (Plunkett Foundation); Nick Plumb, policy manager (Power to Change) on the recently published The Good Councillors Guide to Community Business. The presentation provided a summary of what is a community business, the reasons for the collaborative work and an introduction to the guide.

The presentation was followed by questions and answers. National Assembly members discussed climate change, community assets and encouraging the promotion of the guide.

Alan Collard, adviser (Plunkett Foundation) also shared his involvement with community business from a councillor perspective and encouraging local (parish and town) councils to work together, for the benefit of their communities.

The guide received a positive reception from National Assembly members. Cllr Francis commented on how NALC's policy committee could be involved with identifying any barriers to legislation concerning local councils and community business.

Please click here to access the full presentation (login required).

Resolved: That the guide be received.

<u>NALC committees update:</u>

Finance and Scrutiny:

Cllr Davey spoke to the recent work on Finance and Scrutiny committee. He reported the revised projections of the year end which had indicated a surplus of £13.8k. Cash position is positive. Despite of loss of income, expenditure were under control.

Management Board:

Cllr Drew reported the recent meeting of management board:

- Potential Sale of 109
- Risk Register, noted one county association decline to sign the data sharing agreement.
- Succession planning for NALC committee members and office holders
- Uncertainty of commercial sponsorship
- HR – EAP had been set up for NALC staff

Cllr Blezzard queried if there had been any progress made on NALC presidency to which the chairman responded that this is a work in progress. Cllr Blezzard also asked regarding the discounted membership scheme which Charlotte Eisenhart head of member services will get in touch with him about separately.

Policy committee:

Cllr Francis report the work of policy committee, as well as working on consultations, motions, and the committee had been regularly communicating on the work of:

- Environment bill
- Toilet tax bill

Cllr Francis continued to welcome county association motions and encouraged colleagues to put forward motions, the committee will be considering them.

Smaller councils committee:

Cllr Ford reported the work of Smaller Councils Committee, the committee had a pilot informal meeting which was a success and main purpose of this meeting was to debate the role and function of the committee. These meetings will be taking place more regularly.

nalc
National Association
of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk

w: www.nalc.gov.uk
a: 109 Great Russell Street,
London WC1B 3LD

nalc
National Association
of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk

w: www.nalc.gov.uk
a: 109 Great Russell Street,
London WC1B 3LD

9 March 2021

APPENDIX 4.1 | NATIONAL ASSEMBLY

Updates from Committees

You can access full minutes on the NALC website at:

https://www.nalc.gov.uk/about/governance

Management Board –

NALC's Management Board met on 26 January. Councillors considered the Local Government Association (LGA) model code of conduct and agreed, subject to feedback from county officers, to recommend to National Assembly on 9 March that it be adopted by local councils and replace the NALC code. They stressed that this needed to be part of a wider project on civility aimed at improving standards and behaviours, and agreed on the need to dedicate resources and work closely with the Society of Local Council Clerks.

Finance and Scrutiny Committee

The third quarter draft management accounts indicate that a more favorable variance to budget of Circa £7k will be achieved at the year-end resulting in a £13k surplus at the year-end. This includes the main period for events in quarter four which are expected to breakeven in quarter four.

Other factors contributing to this are the continuing reductions to democracy costs from holding meetings remotely and the continuing effect of increase from affiliation fees due to increased membership.

There is still confidence in commercial income but new challenges mean new approaches as remote meetings do not offer the same experience for sponsors to meet delegates; and some other projects are coming to an end.

The budgets for future years were considered and heads of service noted that they are still comfortable with estimates at this stage which on current trends will result in a deficit of circa £9k for the 2021-22 financial year.

It was noted that recent changes to Exit payment legislation for The local Government Pension Scheme (LGPS) members has been revoked so there is no change, although it appeared that NALC was not subject to it anyway. The latest triennial revue report from the actuaries had been received confirming the NALC contribution would not change in the year-end accounts.

A governance review will take place at the next meeting of the Finance and Scrutiny Committee to revisit the following procedural documents:

- Pensions Explained
- Financial regulations
- The Constitution
- Risk Assessment and Business Recovery
- Financial Overview

Cash balances at this point are healthy and amounted to approx. £494k compared to £474k in the previous year. On current performance at the lowest point of the year our cash position will be circa £300k.

NALC Policy Committee

NALC's Policy Committee held its first meeting of the year on 12 January, here's a summary:

The committee considered a policy motion from the Kent Association of Local Councils on the rights of the travelling community and supported the aim of retaining a balance between the needs of communities and travellers, in the housing policies of local plans. Agreed proposals for NALC's next big theme on young people comprising a dedicated webpage, a case studies publication, events, lobbying for powers and funding, encouraging young people to stand for election and setting up a young councillor's network. Received updates to ongoing work on the planning white paper, local elections and NALC's Make a Change campaign, health and well-being, and climate change including supporting a policy statement by the task and finish group. Noted the publication by the Local Government Association of the Model Code of Conduct which would be considered by the Management Board and National Assembly. Agreed on the importance of Lobby Day to engage with MP's, build relations and raise key national and local issues; and encouraged all county associations and councils to get involved.

NALC Larger Councils Committee

NALC's Larger Councils Committee met on 19 January, here's a summary:

Mark Davies from NALC's partner CCLA gave an overview of the performance of their investments and work on themes including modern slavery, mental health and climate change. The Committee received an update on our lobbying on the Comprehensive. Spending Review and Provisional Local Government Finance Settlement which proposes not extending council tax referendums to local councils. Everyone provided updates on their engagement with MPs and principal councils on funding. Cllr Sandie Webb gave a summary of a paper she had produced in consultation with the Super Councils' Network which covered a range of issues including communications, devolution, finance, procurement, leadership, community governance reviews and recovery planning.

NALC Smaller Councils Committee

NALC's Smaller Councils Committee met remotely on 9 February, here's a summary:

The committee welcomed new members Cllr Bob Blezzard (Isle of Wight) and Cllr Mike Scott (Northamptonshire). It was agreed county association support for smaller councils declaring a climate emergency, would be raised at the next meeting of National Assembly. The committee shared NALC's urgency on ensuring remote meetings are extended beyond 7 May and were keen to emphasise the inclusivity benefit of holding meetings online. Feedback was provided on NALC's guidance on preparing for a return to face to face meetings and consequences of any delay to May's local elections. An update on the Star Council Awards was given and the committee made suggestions on how to attract applications from smaller councils

Governance review working group

Along with many of you, we are beginning to think about how the pandemic experience will affect our working practices in the longer term such as office space and developing our IT and web systems to better support on-line and digital working. A small task and finish group was set up by our National Assembly who met this week and last, concluding that in future we should continue with a mix of face to face and remote meetings and also make greater use of remote meetings to engage with networks of councils and councillors.

nalc

National Association
of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk

w: www.nalc.gov.uk
a: 109 Great Russell Street,
London WC1B 3LD

9 March 2021

APPENDIX 5 | NATIONAL ASSEMBLY

Civility in the sector: NALC position on the LGA's national code of conduct. Joint work with Society of Local Council Clerks (SLCC)

Code of conduct

Assembly members will be aware of representations made by NALC to the Committee on Standards in Public Life (CSPL) enquiry into local government ethical standards calling for a number of measures including stronger sanctions (see background document two below).

Following that enquiry, a number of recommendations were made in the CSPL January 2019 report to the Prime Minister which are still being considered. NALC has written urging the Government to respond to these (see background document 4 below).

One of the recommendations was that the Local Government Association (LGA) be tasked with producing a single code of conduct for local government, which the LGA agreed to do.

NALC has been fully involved in those discussions about the development of that code including through the involvement of a number of county officers. A draft code was produced by the LGA which NALC commented on, including through policy committee, and a number of those suggestions were included in the final edition published by the LGA on the 23rd of December 2020 (see background document 1 below).

The LGA has also commissioned Hoey Ainscough Associates Ltd to produce good practice guidance to accompany the new code of conduct. NALC and other stakeholders have met with them to discuss this and will provide feedback as the guidance is produced.

The new code has been considered by a number of national bodies including lawyers in local government and a number of principal councils have already adopted and are cascading to our sector. County officers have also discussed it and have given it broad support as a step in the right direction.

NALC supported the concept of a single national code, ideally based on its own version, but the new code appears to meet most of our aspirations. Management Board considered this on 26 January and their draft minute concludes:

> "In discussion there was general support for the new code and agreement that it should replace NALC's own code which would no longer be produced. The point was made that NALC's real concern was to see the standards regime have teeth by way of sanctions and other enforcement procedures. These were just as important as the code. It was noted that depending on the supplementary LGA advice there may be need to provide additional commentary and that could be picked up in the light of operating the new code. Noting the opposition of Cllr Francis, the board agreed to propose to national assembly in March that it recommend councils adopt the code and NALC cease to produce its own code."

Accordingly it is recommended that National Assembly be invited to commend the code to county associations and local councils and for NALC to cease the production of its own code.

Wider work with SLCC

As the CSPL noted improving ethical standards in local government requires a wider package of measures than just a code - including sanctions, better training, robust policies and procedures and the involvement of a diverse and broadly experienced cadre of councillors and clerks. Some of these are within the government's remit but many are within the gift of the sector itself. Others, for example the abuse of social media or poor public behaviour towards public servants are of course part of a wider societal problem.

Accordingly the leadership teams of NALC and SLCC will be meeting in March to consider what further steps need to be taken, to produce an action plan and resource its implementation. Regular reports will be made to the Assembly but at today's meeting you may want to discuss what these wider measures may include and how they can be delivered.

The meeting between NALC and SLCC will also be an opportunity to discuss their recent survey of clerks into standards of conduct in councils which shows that around 15% of councils were facing severe behavioural problems. Background document 3 is a letter from NALC's chief executive to the SLCC setting out the association's position.

Background documents:

1. LGA code: https://www.local.gov.uk/local-government-association-model-councillor-code-conduct-2020-0
2. NALC news story: https://www.nalc.gov.uk/news/entry/1500-nalc-calls-on-government-to-introduce-sanctions-to-support-the-proposed-code-of-conduct
3. https://www.nalc.gov.uk/news/entry/1668-nalc-chief-executive-writes-to-clerks-about-civility-in-public-life
4. https://www.nalc.gov.uk/news/entry/1661-nalc-urges-the-government-to-strengthen-standards-regime-to-improve-behaviour-in-councils

2021

THE GOOD COUNCILLOR'S GUIDE TO CYBER SECURITY

This guide aims to help local (parish and town) councils and their councillors better understand the importance of cyber security and provide practical advice on minimising risks to the council. The publication features information on understanding the most common risks and how some simple steps can help protect the council's information and equipment.

CONTENTS

WELCOME

David Astwood
Technical director at
Microshade VSM

As our use and dependency on computers, computerised systems and the Internet grows, so the threat of unauthorised access or malicious damage to, or theft of data from, computer systems is growing at an exponential rate. At the same time there is increased pressure and responsibilities placed on Data Controllers to safeguard personal and sensitive data.

The aim of this guide is to give a high level overview of the types and impact of some of the more common cyber threats that face users of Information and Communications Technology (ICT) today, along with technologies and good practices that can be adopted to protect users and organisations against these threats.

Microshade VSM specialise in the provision of secure ICT systems, specifically designed for the town and parish council market, a market in which it has been active since 1996. Microshade VSM cater for councils of all sizes in this market.

Microshade VSM Local Council Community Cloud provides a secure and ecological managed ICT service hosted from our secure UK data centre. For customers who prefer to keep their ICT local, Microshade VSM provide a suite of appropriate security services to help keep you safe. We have provided informative presentations about cyber security to local associations around the UK, on which this toolkit document is based.

Cllr Sue Baxter
Chairman of the National Association of Local Councils

On behalf of the National Association of Local Councils (NALC), it gives me great pleasure to introduce The Good Councillor's guide to cyber security produced in partnership with Microshade.

I am sure that when most of us decided to become councillors, IT and data security were not at the top of our list of priorities. I suspect that many of us would confess to avoiding such technical matters to focus our time in our communities and on the council's work. This guide aims to show that with just a small investment of time and resource, we can protect our councils from the sorts of risks that could put our work at risk.

I am particularly keen for smaller councils to take cyber security seriously. With many councils having one computer or laptop, the council could suddenly lose years of information and hard work that may never be replaced if that device is lost or compromised. I hope this guide will show how just a few simple steps could help remove this risk and ensure local councils can continue doing good work in their communities without disruption.

During the COVID-19 pandemic, we have seen the vast majority of local councils swiftly move to remote working, with staff working from home and council meetings taking place online. There have been incredible benefits to those changes. Not just keeping everyone safe from the virus but also introducing more flexible working arrangements, making meetings more accessible to the public, and bringing in other innovations to many councils' workings. However, with the increased risks associated with this way of working, we all need to make sure that we are doing what we can to understand and reduce those risks.

Now more than ever, please take the time to consider how your council protects itself from cyber-attacks and other cyber risks. This small investment will pay huge rewards over time as your hard work in your communities is protected for now and the future.

INTRODUCTION

WHY SHOULD I BE INTERESTED IN CYBER SECURITY?

Cyber security is the protection of computer systems from unauthorised access, theft, damage or being made inaccessible. With the growth in popularity of computers, smart devices, the Internet and media sites, there has been a continuous exponential increase in attacks against computer systems with an impact on affected organisations and their reputations.

Information and Communications Technology (ICT) has many benefits, for example enabling organisations to quickly and efficiently publish and widely distribute documentation and other information, advertise events and services, store vast amounts of historical information or correspondence, and communicate with suppliers, the public, and other agencies.

GDPR and the Data Protection Act 2018 require organisations to implement appropriate measures to protect the information they hold, or risk significant fines.

Threats come in many forms and the council must mitigate against a wide range of risks. Disasters can come about from simply dropping a laptop or leaving it or a USB stick on a train, knocking over a cup of tea onto the computer, theft, fire, or sudden loss of a key member of staff who holds the passwords vital to access council information systems.

The council as a whole has a collective responsibility to see that suitable cyber security measures are implemented and supported, and all members of the council must follow good practices to keep their own systems safe.

IT SERVICES PROVIDED BY A PRINCIPLE AUTHORITY

Many local councils have systems (email/website) provided by a principle council, however it remains the local council's responsibility to ensure that their information is managed and secured appropriately. You can make sure the principal council has independent accreditation that shows good security practice such as Cyber Essentials Plus or ISO 27001, or by asking about their cyber security practices using the 10 steps to cyber security guidance.

SMALLER COUNCILS, BIGGER RISKS?

The majority of local councils in the UK fall into this category, with fewer resources and less collective experience available to undertake the necessary steps to implement good safety measures, particularly those employing a lone clerk who works from home, possibly part-time, on a computer that may not be owned by the council.

Some of the problems the smaller council may face include:

- Difficulty in keeping back-up media away from the place of work, which means that the backups could be lost in the same incident that affects the computers (fire, theft, etc).

- The clerk may not have the experience or time to keep on top of cyber security.

- Personal computers could be used for non-council business thus exposing them to unknown cyber risks.

- Business continuity could be compromised if something happens to the clerk's equipment or premises, it may not be possible to access the council's information.

- Succession planning may not be straightforward. If something happens to the Clerk, will the council be able to access the equipment or find the required passwords?

This may all sound scary and overwhelming, but with a small amount of time and effort invested regularly it is possible for councils to manage cyber security risks. This guide provides information on some of the common threats faced by users of ICT and protective measures that can be taken, along with some practical information in the appendix to support you.

YOUR RESPONSIBILITIES FOR DATA SECURITY

Local councils are responsible for the information they hold, whether in electronic form, on paper, or in any other format. Stored information must be protected from unauthorised access, accidental deletion, and malicious hacking attempts.

GENERAL GUIDELINES FOR INFORMATION STORED ELECTRONICALLY

- It should be protected by strong passwords that are never shared.
- If stored on removable media these should be locked away when not in use.
- It should only be uploaded to trusted cloud solutions.
- Servers should be sited in a secure location, away from the general office.
- Data must be backed up regularly, and backups tested.
- Also consider how you protect information on hard disks when equipment leaves the office or is retired.

Many councils find that a small disaster turns into a tragedy when they lose data, then find that their backups have not been reliable.

Tip: regularly test backups by attempting to restore data from them. Backups are the last resort when other attempts to restore a system have failed, and this is not a good time to find out that they have not been working.

GENERAL GUIDELINES FOR INFORMATION STORED ON PAPER

- When not required, papers should be kept in a locked drawer or filing cabinet.
- Do not leave papers where unauthorised people can see them, for example unattended on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. These principles must be “baked in” to your processes at every stage.

The data controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with GDPR, and that these measures are regularly reviewed and updated where necessary.

THE CYBER THREAT LANDSCAPE

HM Government National Cyber Strategy 2016-2021: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

This document talks in plain English (no technical jargon) about the Governments view on Cyber threats and their strategy to counter these.

CYBER THREATS

Cyber Criminals

Increasingly criminals use Information and Communications Technology (ICT) devices to either target other computer systems, or to conduct traditional crimes with increased scale or reach (fraud, bullying, data theft).

State Sponsored Attacks

Most small councils would not expect to be the target of a state sponsored attack, although Government offices are often targeted. However, commonly used ICT and Multi-Media systems which the organisation use may be targeted, for example popular systems like Microsoft Windows or Facebook can be targeted, and councils using these systems could be infected or hacked, unless appropriate protective measures haves been put in place, as described later in this document.

Example: In May 2019 a vulnerability in WhatsApp that enabled hackers to install surveillance programs onto smart phones, was traced back to the NSO Group – an Israeli "cyber arms dealer".

Hacktivists

Issue-oriented individuals or organisations who have an axe to grind or wish to make a statement. For example, perhaps an individual in a community may disagree with a planning decision, and target the council website or computer systems to draw attention to their objection.

Insiders

Threats from insiders can come in various guises. There could be malicious action taken by a disgruntled member of staff, accidental deletion of key information, or even the risk of a key person leaving unexpectedly without passing on critical information.

VULNERABILITIES – WHY ARE THESE THREATS A RISK?

An expanding range of Internet connected "smart" devices

So many devices now have a computing element and are connected to the Internet (Computers, smart phones and tablets, cars, fridges, home management systems, etc), that it gives attackers a wide range of targets.

Hackers may even utilise some of these devices to launch co-ordinated attacks on other computer systems.

Poor cyber hygiene and compliance

There is a lack of skill and training in how to implement and maintain safe systems and good working practices

Legacy and unpatched systems

Many organisations in the UK will continue to use vulnerable legacy systems until their next IT upgrade

Availability of hacking resources

Readily available hacking information and user-friendly hacking tools are available on the Internet and enable those who want to develop a hacking capability to do so.

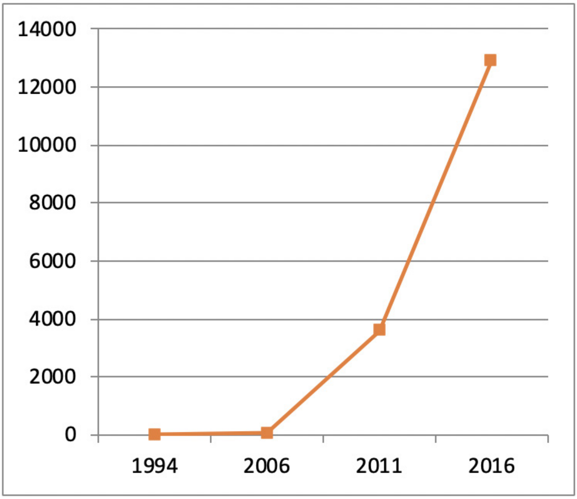
The Growing Threat of Malware

Malware (malicious software), is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. A list of types of cyber-attack and malware is given in Appendix A.

The amount of malware has grown exponentially since personal computers first came into use.

See for Yourself

This shows the staggering number of malware and cyber-attacks detected by Kaspersky Labs, in real time — https://cybermap.kaspersky.com/stats/



In 2019, the AV-TEST Institute registers over 350,000 new malicious programs (malware) and potentially unwanted applications every day, and had registered 928.6 million for the year to August.

HOW IS MALWARE DELIVERED?

What Systems Are Targeted?

Writers of Malware want to make as big an impact as they can, normally in terms of publicity, financial gain, disruption, identity theft, or blackmail. To this end, they target systems or organisations which, if successfully compromised, will give them the biggest returns. They often target:

- Common computing devices or popular apps and games. For example, the WannaCry virus targets Windows 7 computers. In May 2017 an estimated 300, 000 devices were infected worldwide.

- Banks and financial institutions. For example, in Sept 2017 Equifax, a US Credit Agency, was hacked. 143 million accounts were stolen including customer social security numbers and driver's license numbers.

- Social media sites with many user accounts. For example, the WhatsApp vulnerability of May 2019 was estimated to impact a potential 1.5billion users.

Malware Delivery

The most common ways of delivering Malware are:

- Emails. By far and wide the most common delivery mechanism is emails containing links to malicious website programs, or attachments containing malware.

- Popular Websites and Multimedia Sites. If a hacker can put malicious code on a popular multimedia or web site, for example Facebook or the BBC Good Food Recipe site, it could still be run by thousands of visitors in just a few minutes.

- USB Drives. USB drives are a very effective way to deliver malware directly to the computer, by-passing firewalls and spam filters, and are a cyber-security problem in many ways.

Apple Macs and Linux Systems Are at Risk Too

Malware and cyber-threats are not limited to Windows systems. As Apple Macs and Linux systems gain popularity, they too are being targeted (Kaspersky Labs identified over 6 million attacks against Apple Macs in 2015).

These systems can be vulnerable to direct attacks, or used as hosts on which Windows viruses can reside and be distributed to Windows computers.

COMPUTER DEVICE AND NETWORK PROTECTION

ANALYSIS OF AN ENCRYPTION VIRUS DISASTER - WANNACRY VIRUS AT THE NHS

In May 2017, the WannaCry virus infected many computers across the NHS (and other organisations), which encrypted any and all files accessible from the infected computer account. Patient records, operating theatre timetables, and other records were made unavailable so that many NHS services ground to a halt. The Daily Telegraph reported that 19,000 appointments had to be cancelled costing the NHS £20m, and the clean-up operation cost a further £72m.

By looking at what we know about the WannaCry virus, and reports from the time, we can build a picture of what vulnerabilities were exploited, and learn to prevent this sort of thing happening at our local councils.

Further reading: National Audit Office report: WannaCry cyber attack and the NHS — https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

ENDPOINT SECURITY

Endpoint Security is a suite of technologies that are designed to protect your computing device from a variety of cyber threats, for example malware, software vulnerabilities, malicious websites, unauthorised access or

1

The WannaCry virus was delivered as an attachment or link, in an email, to recipients at the NHS.

A good spam filter would be expected to filter out malware before it is delivered to a recipient's Inbox. However, be warned that spam filters are never 100% effective.

2

Recipients opened an attachment from an email received from unknown senders. The malware is activated.

It is risky to open attachments or click links in emails unless you check with the sender first – even if the email appears to come from a known sender. Computer users need training to spot dangers online. Good training develops safe working practices.

3

Anti-malware did not stop the application from encrypting files and folders, or from spreading.

A good anti-malware program should know that applications are not expected to encrypt files and folders, and should have put a stop to this. There is further advice on how to choose a good solution later in this guide.

4

A vulnerability in the Operating System allowed the malware to run with system permissions.

Microsoft had released updates which closed the vulnerability 2 months before the NHS were infected, and published details in computer press 1 month before the incident. Always update your computer and software as soon as possible as they are released.

5

Press reports at the time indicated that some records could not be recovered.

Test your backup systems regularly (every month or quarter), to confirm they are working correctly and that you can restore the information you need to protect.

program execution, and more.

Choosing good endpoint security

There are many competing Endpoint Security products on the market, offering a variety of protection technologies, and you must choose the right one according to your needs and budget. Examples of the choices you can make may be:

- Data Encryption: you may need this if you have a portable device, such as a laptop or smartphone, if your Operating system does not already provide this function.
- Backup: some Endpoint Security offer file backups as part of the package, if you don't have another solution in place.

Tip: Look for "Real-Time Protection" or equivalent technology. This technology recognises the normal behaviour of common applications, and if it detects the application doing something unusual it will put a stop to it. This should protect against encryption attacks and many newly emerging threats.

Independent Endpoint Security testers

Free and independent Endpoint Security testers' websites show results from regularly testing of the security products on the market against emerging cyber threats. Visitors can use this information to see what products are performing well, and have been performing well over a period of time, to help select a product with a reliable history of good performance.

Tips:

1. New computers often come with trial protection software pre-installed. This does not mean that the protection software is good, so much as that the software manufacturer has a distribution deal with the computer manufacturer. Check the reputation of pre-installed protection software with an independent test site before committing to it.

2. Look for “Real-Time Protection” or equivalent technology. This technology recognises the normal behaviour of common applications, and if it detects the application doing something unusual it will put a stop to it. This should protect against encryption attacks and many newly emerging threats.

3. Look for “behavioural analysis”. This technology recognises anti-malware by the way things it does, for example, an encryption virus will first load a list of all files it can find into memory, ready to attack them. This is another technology that can protect against newly emerging threats.

Configure your Endpoint

Check that you have installed a license. Check that the solution will do a full system scan at least once a week. Plan to check back regularly to see that your solution is still working correctly.

Test your Endpoint Security

Use a reputable website to download benign files that contain virus signatures designed to trigger your anti-malware without causing damage. This not only demonstrates whether your systems are protected, but provides an opportunity to see and perhaps plan for what will happen, in the event of a real incident.

SYSTEM UPDATES

Hackers look for bugs or vulnerabilities in the Operating System which allow them to e.g. learn your user names and passwords, and send these back to the hacker. Operating System updates are written by the manufacturer (Microsoft, Apple etc.) to close these vulnerabilities or mitigate the risks, and must be applied regularly and as soon as they become available.

Check System Update Status

Plan to check periodically that updates have been running regularly and successfully:

- Windows 8-10: open the Settings App (from the start menu), and select “Updates and Security”.
- Apple Mac: Open “System Properties” from the “Apple” icon
- Linux: check the recommended procedure for your Linux variant. A regular update task can be configured as a scheduled (cron) job.

APPLICATION UPDATES

Applications are the programs on computers that are used by the computer user, such as word processors, spreadsheets, web browsers, etc. Vulnerabilities in the applications are equally useful to hackers, and the writers of the applications publish updates to address these risks.

Periodically review the software programs installed, making sure they are up to date. Software programs which are no longer used or supported should be removed.

There are software tools on the market (often part of your Endpoint Security) which will audit your computer periodically and notify you of any software updates that are required, and manage the update for you. Be sure to choose a reputable provider.

THE RISK OF UNSUPPORTED SYSTEMS AND SOFTWARE

If you are using unsupported operating systems or programs, security updates for these products are no longer provided and users are at an increased risk of cyber-attack. Plan to upgrade your systems.

These products are unsupported or near end of support: Windows XP, Vista and Microsoft Office 2007, Server 2003, or earlier are unsupported. Windows 7, Microsoft Office 2010, Server 2008, Server 2008 R2 are unsupported from January 2020.

USER ACCESS CONTROL

User Account Control (UAC) is a security feature of Windows which helps prevent unauthorized changes to the operating system.

Check that UAC is not disabled, and pay attention to any un-expected prompts from UAC that may indicate malicious activity by a software program.

WI-FI AND SMARTPHONE TETHERING

Wi-Fi uses radio signals to connect your devices to the Internet, via an internet router which supports Wi-Fi. Smartphone users have a similar option which enables the computer to connect to the Internet via the Smart Phone's telephone service, again via using radio signals.

Anybody in range could potentially intercept those radio signals and see everything you are doing on the

Internet, staling your passwords or sending you malicious information in place of the legitimate web service.

This is particularly true of operators of Public Wi-Fi as all your Internet traffic passes across their routers and could be re-directed to malicious sites of the operators choosing.

VPN – VIRTUAL PRIVATE NETWORK

A Virtual Private Network ensures that your communications are encrypted between your device and your service provider:

- Your communications are not readable
- Your location is not traceable
- Your ISP cannot track your Internet history

VPN services can be purchased and downloaded on-line for computers and smart devices, and some Internet routers support a VPN service which would protect all devices that are connected to the router.

FIREWALLS

A firewall is usually part of your Internet router and/or may be installed on your computer. The firewall prevents unauthorised access into your organisation's network from the Internet (while allowing your authorised users to access the Internet). Some firewalls also have very sophisticated tools built in that can block spam or malware (inbound or outbound), restrict what websites users can access, and many other things.

Firewall Checks

Common problems with basic firewalls are:

- The administrative password has not been changed from the default password that was shipped with the device, enabling hackers to take control of the firewall and access any devices protected by it.

- The firewall is out of date or no longer supported. Check your firewall firmware or operating system and update it when a new version is available. Replace unsupported devices.

- Ports have been opened enabling access from the outside (see below). Hackers will quickly find these ports and start to probe to find what they can access.

Firewall ports

- Firewall ports enable network administrators to control which services on the local network can be accessed from the Internet. Each port has a number according to the sort of service that is usually available on that port. Common port numbers are 21 (file transfer), 25 (email delivery) and 80 (web server)

- If you have an email server on your network, for example, you would open port 25. Unused ports should be closed.

Check What Ports Are Open in your Firewall

Open your Internet browser and search for "What's My IP", and open a site which will report your IP address, for example https://www.whatismyip.com/

Example: The website will return an IP address number like 76.145.213.195

Use the above number on a port scanning site, for example https://hackertarget.com/nmap-online-port-scanner/ to see what ports are open.

Review any open ports and close any that are not needed. Your router administration guide or internet service provider (ISP) should show you how. Router administration guides are often available online.

SMART PHONES AND TABLETS

Smart phones and tablets are increasingly used in all areas of business. They can learn and hold large volumes of sensitive information about the owner and their contacts, access work data and services, connect to unsafe networks, and are inherently losable, attractive to thieves, and vulnerable to hackers and malware. Protect these devices like any other computer:

- Use a strong password or PIN
- Think before installing Applications, and be suspicious when applications want to access data for example contacts
- Use security / anti-malware software
- Keep the Operating System and Apps up to date
- Set up device tracking and remote wipe
- Enable device encryption
- Make sure you are running backups
  - Be wary of public Wi-Fi

BACKUPS

Disaster can strike causing loss of data despite anyone's best efforts to protect the computer systems, leaving computer users only one course of action – to restore from backup.

Be Prepared to Restore Your Data

- Periodically review and double check the data you need to include in your backups
- Think about backup retention – how long the backup is kept before it is overwritten
- Take regular backups – any work done since the last backup will need to be re-done.
- Monitor backup reports and address problems
- Store backup media safely at a location remote from the systems, to avoid the systems and the backups being lost together in a fire or burglary.
- Periodically check that you can restore files from your backups.

It can be difficult for small councils to store backup media away from the place of work. For computers located in the office, the clerk may be able to take backup disks or tapes home when not in use. If the main place if work is the clerk’s home, then nominate a councillor to hold the backup media.

Backup Retention

Backup retention means how long is a backup kept, before it is overwritten. Ask yourself "If a file or folder is accidentally deleted, corrupted or overwritten today, how long do you want to allow for someone to notice there is a problem and still be able restore it from a backup". You will want enough backup disks or tapes stored to allow you to go back your preferred period in time.

An example backup retention policy is given in the Appendices of this guide.

CYBER LIABILITY INSURANCE

You may need cyber and data risks insurance if you:

- hold sensitive personal data, such as names, addresses or banking information
- are reliant on computer systems to conduct your business
- have a website
- are subject to a payment card industry (PCI)

merchant services agreement

There are several insurers that specialise in the town and parish council market. In addition to a financial re-imbursement, some offer additional professional services which might be essential in the event of an incident, for example advice on finding ICT professional help to recover data, communications assistance to deal with affected contacts and the press, and so on.

PORTABLE DEVICES, USB DRIVES AND ENCRYPTION

USB drives or memory sticks pose serious security risks in terms of malware delivery, and along with any portable drive or device are a risk of data loss or data breach.

Malware Delivery with a USB Drive

Malware delivered on a USB drive by-passes the usual first lines of defence (firewalls and spam filters).

When someone plugs a USB drive into a computer, the computer looks for program information on the drive. If a hacker puts their malicious code onto a USB stick, it would be executed automatically when the USB drive is plugged into a computer.

Researchers have shown that on finding a USB drive, many people will instinctively plug it into their nearest computer to see what is on it, not realising that this will automatically run any malicious code that might be on there.

Data Breach with a USB Drive or Portable Device

USB drives and other portable devices are easily mislaid, stolen or broken, and should be encrypted to protect against accidental loss and data breach.

Sensitive information (for example personal data, such as names, addresses or banking information) should:

- Never leave the organisation's secure computer system.
- Not be put onto USB drives or portable devices, which are easily mislaid.
- Be protected by encryption, if on portable drives or devices.

Example: Serious data breach from USB disk: https://www.bbc.co.uk/news/business-45785227

Encryption to Protect Your Data

Encrypted files are encoded rendering them unreadable to anyone who does not have the pass code or key.

Any portable media or laptops leaving the organisation premises should be encrypted to protect sensitive data on them. Disk Level Encryption ensures that the Operating System is all encrypted and cannot be booted without the key. This protects your device from hackers who can crack your Windows password (which is often quite straight forward!).

Windows Pro editions come with encryption software called BitLocker built in, or 3rd party encryption software is available.

EMAIL SECURITY

COUNCILS CAN BE EASY TARGETS

It is very easy for cyber criminals to send an email and make it look like it comes from someone you know and trust. Councils are easy targets because:

- They publish information about their activities, employees and councillors online, helping spammers to target or impersonate individuals in the organisation, and using insider information to make fraudulent emails sound plausible.

- Recipients of council emails (residents, councillors etc) often use free email accounts from popular providers (which are targeted by hackers), and easily cracked passwords or poor security practices.

SPAM

Spam is electronic junk mail or newsgroup postings, usually unsolicited. Approximately 50% of all emails sent are spam. Spam can be just annoying, but often contains malware, links to malicious websites and phishing links, or attempts to impersonate known contacts in order to defraud the recipient.

What are Spam Filters?

Spam filters are designed to prevent spam from being delivered. Spam filters can operate in several places, for example:

- Your email client (for example, Microsoft Outlook) may put spam in the Junk folder. The problem is that the spam is now on your computer and could accidentally be opened.

- Your mail server (the server where your emails arrive, which may belong to the council or to your email service provider) or firewall may intercept the spam before it is delivered to your mail client. This is better but still the malicious email is on your network.

- A cloud based spam filter can filter spam before it ever reaches your network.

Spam Filters - Necessary but Fallible!

Spam filters can remove a lot of unwanted or malicious spam, but they are just computer programs that aim to identify spam according to the content of the email – where the email came from, the words used, whether there are attachments or links inside, and so on.

Cyber criminals spend their time designing malicious emails that will get past any spam filter. For example, a recent trend is to send an email containing a link to a clean webpage (which they own), which will get though most spam filters. Once the email has been delivered, they change the webpage content to something malicious, to infect the computer of anyone who clicks on the link.

Choosing a Good Spam Filter

As with all things, there are many spam filters available with various protection technologies and other features. Make a decision based upon whether you want the spam filter in the cloud, or on your local system, budget, and protection offered. Look for some of these features:

- High rate of detection.
- Low rate of false positive detection (legitimate emails blocked as spam).
- Malware filtering.
- Anti-phishing link protection (both pre- and post-delivery).
- Protection for outbound messages (prevents your mailbox being used by spammers, if compromised.

Guard Your Users Against Spam

Inevitably, some spam will get through any spam filter. Be suspicious of emails which:

- Contain links or attachments, whoever it is from (it is easy for a hacker to send an email that looks like it comes from a trusted contact)

- Come from someone you don't know

- Comes from a known contact but

  - Is asking for money or personal information

  - Does not use the sort of phrases that person normally uses

- Contains spelling or grammatical errors (the sender's first language is often not English)

- When you open an attachment, if it prompts you to "enable Macros", it is trying to run another program in the background. This is probably malicious

Tips:

1. Hover over the sender's address to see who really sent the email.

2. If there is a link in the email, hover over the link to see the website it really points to.

PROTECTING THE COUNCIL'S EMAIL REPUTATION

Email reputation is important. Reputation is based upon whether your email server or email addresses have been reported as sending a lot of spam. Senders with bad reputations will find that the emails they send are more likely to be treated as spam, ending up in people's junk folders. Sender's with especially bad reputations will be blacklisted, which means that recipient email systems will refuse to deliver your emails at all.

Bulk Emails

It can be embarrassing and difficult to resolve if a council's email domain is blacklisted. However this can happen even if staff or officers have been sending what they believe to be legitimate emails, but which automated spam filters detect as spam. Common habits employed by councils which trigger spam filters include:

- Sending bulk emails (sending an email to dozens or hundreds of email recipients).

- Sending emails which contain links or pictures which contain links, and especially if these links go to pay sites.

An example might be the case of a council which wants to advertise an upcoming event, and so includes an email footer on all outgoing emails with a picture advertising the event, which contains a link to a site where tickets can be purchased. These can soon trigger spam filters, especially when emails are sent in bulk.

To avoid getting blacklisted, it is a good practice to use an online bulk email service, to send emails to multiple recipients or for advertising, or the Gov.UK Notify service.

Gov.UK Notify service — Councils with a .gov.uk email address can send an unlimited number of emails for free with the GOV.UK Notify service : https://www.notifications.service.gov.uk/

Securing government email

This guidance applies to all email domains that public sector organisations run on the internet.

Central government require all government organisations to secure their emails following guidance on their "Securing government email" web page. You must:

- Encrypt and authenticate email in transit (see below)
- Use extra encryption if your data needs more protection – for example if the content contains sensitive or personal information that should only

be read by trusted recipients.

- Make sure the recipient protects the data you send to them by complying with standards such as Cyber Security Essentials (explained later in this guide) and GDPR.

- Make email security invisible to end users as far as practically possible – in other words the email system really should make emails secure without the user needing to take extra steps

Encrypt and authenticate email in transit

As this is quite technical, councils may need to involve their email mailbox provider to configure their email systems appropriately, although there are guidelines accessible from the Securing government emails website

1. TLS (Transport Layer Security): Your email system must use TLS version 1.2 or later for sending and receiving email securely. This encrypts your emails so they cannot be read in transit. This is a function of the email server that you use to send the email.

2. DKIM (DomainKeys Identified Mail): adds a unique encrypted signature to your outgoing email. The receiving system can check the signature against the received message contents to ensure that the email

has not been tampered with in transit.

3. SPF (Sender Policy Framework) records must be published on your domain which inform receiving mail systems which mail servers are authorised to send emails from your domain. Emails from your domain that are received from other servers are treated as spam.

4. DMARC (Domain-based Message Authentication, Reporting and Conformance) records must be published on your domain, advising receiving systems how to validate emails from your domain, and what to do or who to inform, if non-compliant emails are received.

POLICIES, STANDARDS AND TRAINING

VULNERABILITIES INTRODUCED BY COMPUTER USERS

“There is no conceivable information security system that can stop one person out of a hundred opening a phishing email, and that can be all it takes.” — Ciaran Martin, Director General for Cyber Security, GCHQ – June 2015 (source: HM Govt National Cyber Strategy 2016-2021)

No matter how much technology is in place to protect our computer systems, the weakest point in an organisation’s security is often the person using the computer, who can be persuaded to undermine their security systems for many reasons.

Examples of how human vulnerabilities are exploited include:

Desire to be rich / to get something for free

- You’ve won! Click here to claim …
- You’ve paid too much tax …

Paranoia or Gullibility

- This is Microsoft – I need to help you fix a problem on your computer

- Your mailbox is full and cannot send more emails. Click here and enter your mailbox password to clear it

Need for Sociability

- Can I be your online friend?

Careless typing

- Many variant spellings of google.co.uk that land on malicious websites!

Inquisitiveness

- We failed to deliver your parcel – please click here ...
- Shocking celebrity pictures ... click here

TRAINING AND OTHER USEFUL SOURCES OF INFORMATION

There are numerous training resources available to computer users and which could become part of a personal development plan. Sources include:

Kaspersky Automated Security Awareness Training10 is an online training and certification programme, requiring about 15 minutes per week, which builds safe practices as habits.

The International Computer Driving License is an organisation which offers a range of ICT and cyber security modules and programmes covering from the basics to more advanced subjects.

Kaspersky Labs' Advanced Security Awareness Training is an on-going online training curriculum teaching good behaviour through simulation and repetition. It adapts to a user's role and experience, provides management reporting and can be useful to demonstrate an organisation's commitment to cyber security, which is useful in the event of an incident which the Data Commission may need to investigate. Available through Microshade VSM.

CYBER SECURITY ESSENTIALS

National Cyber Security Centre "Cyber Essentials" website provides up to date guidance on how to keep safe as well as the Cyber Security Essentials programme, which is a certification programme which enables holders to demonstrate that they are working to secure their ICT systems against cyber-attack.

CYBER SECURITY SELF-ASSESSMENT

The LGA recently launched their cyber security self-assessment tool which will halp you assess your security readiness.

ICT POLICIES AND PROCEDURES

Councils should implement, enforce and maintain good policies and procedures to govern and guide users of their ICT resources and data. Example policy templates can be obtained online, or from HR and other business management consultancies.

ICT Usage Policy

This policy should advise staff, officers, and councillors on appropriate use of council equipment and information for, as well as what is inappropriate and should answer questions like:

- Who retains ownership of information created by staff or officers which they have stored on council equipment, and which may be personal in nature

- Is it appropriate for users to use their own devices, and in this case how is information stored on these devices, and what happens when the owner is no longer associated with the council?

- If equipment or mailboxes are provided to councillors in order that the can perform their duties while in office, who retains ownership of these things, and what happens to any information held in mailboxes or on hard disks?
- What level of cyber security training should be reached for users with access to council emails or computer systems (staff, officers and councillors)

Password Policy

The National Cyber Security Centre document "Password administration for system owners" contains up to date information on good practices for your passwords. Where passwords are employed, the advice is to use a stronger password, but change it less regularly.

A password policy needs to address, among other things:

- How complex must passwords be, and how often must they be changed?
- Is an account locked after a number of bad password attempts, and how is it then unlocked?
- What is the procedure when a staff member leaves,

to remove their system access?

- Ensure that users have no more system access than necessary.

Tips:

1. Avoid using the same password on multiple systems, especially online – if a hacker cracks your password on one system, they will try the same password on other common services.

2. Search the Internet for commonly hacked passwords, and avoid these.

Incident Response Procedures

Who takes what steps in the event of an incident? For example, if a computer is infected with a virus, the user should probably remove it from the network immediately before the virus spreads further.

Equipment Maintenance and Safe Disposal Procedures

How to keep ICT equipment running safely and securely, and how to dispose of it securely when it is no longer used.

APPENDICES

SECURITY SERVICES FROM MICROSHADE VSM

For more information please see our website: www.microshadevsm.co.uk

Local Council Community Cloud

Microshade VSM's flagship service is the "Local Council Community Cloud" with significant benefits for councils over Office 365. Our suite of managed services is developed specifically for the local council market, delivered from servers located in the UK, and accessible securely over the Internet.

The Local Council Community Cloud removes both applications and data from your vulnerable local computers, and addresses numerous issues commonly faced by councils, including:

- Business Continuity and Succession Planning
- Protection from malicious actions
- Cyber Security issues under Data Protection Regulations
- Data back-up compliance
- Flexible and secure working, from any location

(remote sites linked as standard)

- Data and applications located in a secure environment situated in a UK Data Centre
- Simplifies compliance with Data Transparency Code requirements
- Ecological and cost saving, reducing the need for continuous re-investment in equipment
- Fully supported
- A full suite of appropriate applications for all a council’s needs
- Suitable for smaller councils as well as larger councils

Electronic Document Management

Quickly scan paper documents and incoming post into our secure, online filing system. Configure the system to automatically file documents according to their type (bills and invoices, meeting minutes, etc). Advanced document retrieval tools enable instant document retrieval.

Managed Desktop Security

Managed Desktop Installation Server – upgrade all computers to a clean Windows 10 in minutes, with managed Endpoint Security pre-installed. Managed operating system and application updates, application whitelisting option, drive encryption option, and wipe hard disk before disposal.

Managed Endpoint Security - installation of a leading Endpoint Security product, centrally managed and monitored by our technical support team.

Managed Android Endpoint Security - installation of a leading Endpoint Security product, centrally managed and monitored by our technical support team, including track, lock, or wipe of lost devices.

ICT security audit - inexpensive security MOT for your computers.

Other Products and Services

Kaspersky Advanced Security Awareness Training

Email Spam and Virus filter – filter spam and viruses in the cloud, before they are delivered to your mail server or Inbox. Includes Impostor protection and Anti-Phishing pre- and post-delivery.

Mailboxes – full Microsoft Exchange email mailboxes (compliant with government requirements).

GDPR pack – GDPR templates and procedures, consultancy, outsourced DPO.

SUGGESTED SECURITY SCHEDULE IN THE OFFICE CALENDAR

Annually

Endpoint Security license renewal

Review Policies and Procedures

Review staff cyber security training

Monthly or Quarterly

Endpoint Security checks:

- Endpoint Security product is still supported
- Update Endpoint Security version to the latest version
- Endpoint Security on all systems reports that it is

operating correctly

- Benign virus tests (eicar.com or wicar.org)
- Definitions are up to date
- Full system scan scheduled weekly
- Review logs

System Updates checks:

- Check all equipment including computers and servers, Internet routers, firewall routers etc
- Operating system is still in support? What is the End of Support date? Retire and replace systems which are out of support
- Check automated system updates are up to date
- System updates are scheduled to run regularly (at least weekly)
- Review logs

Application Updates checks:

- Application is still in use? Uninstall unused applications

- Applications still in support? What is the End of Support date? Uninstall unsupported applications

- Applications updates are up to date? Update out of date versions

Backup review

- Test that you can restore data from your backups

- Check that you are backing up everything you should be

RETENTION POLICY EXAMPLE

This example is based on the "Grandparent-Parent-Child model", which allows the following:

- Recently corrupted or lost files can be restored to the state they were in from any day over the last week.

- Files that were corrupted or lost a longer time ago can be restored from the state they were at the end of any week over the last month, or from the beginning of any month for the last quarter.

You will need the following backup media (tapes or disks according to your system):

- 2 sets of media labelled "Daily Set 1" and "Daily Set 2".
- 4 sets of media labelled "Week 2", "Week 3", "Week 4" and "Week 5".
- 3 sets media labelled "Month 1", "Month 2", "Month 3".

Carry out your backups according to the table below. At the end of each week, take that week's daily and weekly or monthly media off site until they are needed again.

Differential vs. Incremental backups

Full backups back up all your data, but this is time consuming and uses a lot of backup media.

Differential backups save on the amount of media you need. Differential backups only save any changes since the last full backup. On Monday, anything changed on Monday is backed up. On Tuesday anything changed on Monday or Tuesday is backed up, etc. To restore data from Tuesday, you need the last full backup media, plus the Tuesday media.

RETENTION POLICY EXAMPLE

Day	Media label	Backup type
1st Friday of Month	Month 1	Full backup
Tuesday-Sunday	Daily Set 1	Differential (changes since the last full backup)
2nd Friday	Week 2	Full backup
Tuesday-Sunday	Daily Set 2	Differential (changes since the last full backup)
3rd Friday	Week 3	Full backup
Tuesday-Sunday	Daily Set 1	Differential (changes since the last full backup)
4th Friday	Week 4	Full backup
Tuesday-Sunday	Daily Set 2	Differential (changes since the last full backup)
1st Friday of Month	Month 2	Full backup
Note – from this point start re-using media		
Tuesday-Sunday	Daily Set 1	Differential (changes since the last full backup)
2nd Friday	Week 2	Full backup
Tuesday-Sunday	Daily Set 2	Differential (changes since the last full backup)
Etc		

Incremental backups save even more space on your media by backing up only changes from the last full or incremental backup, whichever was most recent. On Monday, files changed on Monday are backed up. On Tuesday, files backed up on Tuesday are backed up but files changed on Monday are not. To restore data from Tuesday you need the last full backup media, plus the Monday and Tuesday media. This is time consuming and if any backup media in the sequence is lost or corrupted, you will not be able to restore from backups after that date.

TYPES OF CYBER ATTACK AND MALWARE

Types of Cyber Attack

- Backdoor – a method that allows security to be bypassed – perhaps built in by software vendor
- Denial of Service – prevents legitimate users from being able to work
- Direct access – accessing the target computer directly
- Eavesdropping – intercepting communications between one computer and another
- Spoofing – a malicious system which masquerades as

another, trusted system

- Phishing – an attempt to have the user disclose sensitive information such as passwords or credit card details, normally via email
- Clickjacking – invisibly overlaying a malicious website over a trusted website in order to intercept user input
- Social engineering – aim to fool a user by impersonating a contractor, bank representative, etc

Types of Malware

- Viruses/Worms - software which can copy itself and insert itself into other programs, usually for malicious purposes
- Trojan Horse - a program which appears innocuous, helpful or interesting in order to persuade a user to install it
- Adware – delivers annoying advertisements
- Spyware – collects data and keystrokes including passwords and sends it to a 3rd party
- Ransomware - encrypts sensitive data and demands

a ransom for its release, otherwise the data is deleted

- Bots - programs designed to automatically carry out specific operations. Large numbers of infected computers can be manipulated to conduct a synchronised "Denial of Service" attack

- Rootkits - install themselves deeply into the Operating System in order to remain hidden

- Backdoors - a method that allows security to be bypassed – perhaps built in by software vendor

RESOURCES

10 steps to cyber security	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12
Guide to the General Data Protection Act	https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
AV test Institute	https://www.av-test.org/en/statistics/malware
AV Comparatives	https://www.av-comparatives.org
AV Test	https://www.av-test.org/en
Eicar	https://eicar.org
Wicar	https://wicar.org
Securing government emails	https://www.gov.uk/guidance/securing-government-email
Kaspersky Automated Security Awareness Training	https://www.microshadevsm.co.uk/cybertraining.php
International Computer Driving License	http://ecdl.org
Cyber Essentials (NCSC)	https://www.cyberessentials.ncsc.gov.uk

RESOURCES

LGA Cyber Security Self-Assessment	https://www.local.gov.uk/our-support/efficiency-and-income-generation/cyber-security/cyber-security-self-assessment-tool
Password policy: updating your approach (NCSC)	https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
Password administration for system owners (NCSC)	https://www.ncsc.gov.uk/collection/passwords
Small Business Guide: Response & Recovery (NCSC)	https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

NOTES

NOTES

NOTES

NOTES

Published by National Association of Local Councils (NALC)

109 Great Russell Street
London
WC1B 3LD

020 7637 1865
nalc@nalc.gov.uk
www.nalc.gov.uk

Every effort has been made to ensure that the contents of this publication are correct at the time of printing. NALC does not undertake any liability for any error or omission.

NALC cannot be held responsible for the failure of advertisers to provide the services or products advertised.

Other publications in The Good Councillor's guide series are available:

The Good Councillor's guide

The Good Councillor's guide to neighbourhood planning

The Good Councillor's guide to finance and transparency

The Good Councillor's guide to transport planning

The Good Councillor's guide to community business

The Good Councillor's guide to being a good employer

National Association of Local Councils (NALC)
109 Great Russell Street, London WC1B 3LD
t: 0207 637 1865 e: nalc@nalc.gov.uk w: www.nalc.gov.uk

nalc
National Association
of Local Councils

TASK AND FINISH GROUP

NALC GOVERNANCE

MEMBERS

The team:

- Phil Harris (apologies for meeting one)
- Lillian Burns
- Elizabeth Luder
- Ken Browse
- Peter Allison
- Mike Scott
- Mike Drew
- Tony Howard (apologies for meeting one, e mail comments submitted)

FIRST MEETING – 28/01

Question one:

- How do you think that the remote meetings we have held at NALC have worked?
- Have they enabled you to contribute to the oversight and development of the Association and It's policies?
- Are there any particular technology issues that you face.

Some initial thoughts:

- Generally gone well and able to contribute (connectivity an issue for not spots) - Tony
- NALC remote meetings too short. Could encourage informal engagement by opening zoom earlier - Lillian.
- Training session on how to host remote meetings - Lillian
- Remote meetings may have worked well but are the meetings themselves fit for purpose? - Mike
- Better use of polling to get view from floor - Mike

FIRST MEETING – 28/01

Questions two:

- If the answer to the first question is broadly positive is there scope to develop the use of remote sessions further as the pandemic eases? For example might we want to continue with a hybrid approach to committee and assembly meetings of an occasional face-to-face supported by more frequent remote meetings?

Initial thoughts:

- In Lincolnshire there is an idea awakening that meetings would best move forward in a hybrid form. Geography especially in Winter! Preliminary view regular meetings being by Zoom but longer events (Conference) face-to-face. - Tony
- Remote TFGs work well - Tony
- Cannot return to face to face until safe to do so - Lillian

FIRST MEETING – 28/01 NOTES

The group outlined the aim of the Task and Finish Group – To gain feedback on how remote meetings have worked, to discuss technological/practical issues and group to make recommendations to Assembly on the associations approach to meetings post pandemic.

Remote meetings:

Remote meeting have been well received so far but scope to build in better engagement in the meeting such as use polls, reactions etc and build in feedback during the meeting. They can include people who may otherwise feel excluded because of travel constraints or shielding. As a contra some people are attracted to involvement because of engagement in London

Length of meetings:

The group asked if further time can be built in for the committee meetings as one hour is not sufficient. Build more time for comfort breaks before and after the meeting. Maybe meet more frequently rather than longer. HSE advice?

Technology:

Beware of poor broadband and interruptions. Some councillors may need support in terms of equipment, Wi-Fi or training. An allowance?

Post pandemic:

Association will aim to support hybrid approach where there will be a mix of face to face/remote meetings with balance towards remote meetings. More scope to have networks rather than having formal meetings. Broad support for 1 face to face to 3 remote meetings

SECOND MEETING – 04/02

Questions three:

- We have been able to develop the use of more informal networks and networking opportunities because of the reduced costs of transport and accommodation etc. For example the informal assembly meetings, committee meetings and networks such as the super councils network and our more regular monthly remote conferences have reached a wider audience. Does this model enable us to reach out to more councils and engage more widely with colleagues across the country?

Initial thoughts:

- Open up NALC meetings to observers? - Tony
- Has widened attendance/involvement - Lillian
- Has NALC centre the resources to support more informal events? Keen to have event for smaller councils. - Lillian

SECOND MEETING – 04/02

Question four:

- Views on how NALC communicates with you via e mails etc. in your role as Assembly member, in terms of distributing information and papers. How can it be improved?

Initial thoughts:

- Merge LCE into LGA magazine - Lillian
- Ensure councillors are digital savvy
- Send reminders on day of meetings with joining details – Phil
- Send out calendar invites from outlook for meetings - Phil

nalc

SECOND MEETING – 04/02 NOTES

Informal meetings: The group agreed this model would work and enable the association to reach out more widely with colleagues across the country, would endorse on holding more informal meetings between assembly members and CALC colleagues. More brainstorming sessions should be held informally in preparation for the actual meeting. Important to use informal meetings for assembly members to get to know each other before elections. Use breakout rooms

Resources for network groups: The group asked if resources would be allocated to facilitate the network groups as they would need be monitored and managed properly. If formal meetings are reduced, more staff and resources could be provided.

Post-pandemic: Have a mix of face to face/remote meetings, rather than following a strict structure, issues or matters can de dealt with when they first come, this model would allow to be more productive. Any decisions can be reported back to the committee.

Website uploads: The group discussed how to improve on signposting appropriately to the website, it would be helpful to have a direct link to the page rather than members having to search. It was agreed to not have attachments to emails but rather have a Dropbox or one share option. NALC are currently carrying out work to improve the website.

Communications: It was agreed for NALC to continue using committees inbox for committee related communications and refrain from using officers email address. In addition to this, the group stressed that screen share should be used more regularly during meetings to share agenda, papers etc.

Distribution of papers: The group agreed to work towards a paperless model and digitalising papers, make more use of the website. Although some members asked if long reports could be sent to assembly members via post as they are difficult to navigate. Send out reminders day before the meeting with agenda and papers.

SECOND MEETING – 04/02 – ADDITIONAL POINTS

- Policy committee to use informal zooms to quickly discuss government consultations
- Informal coastal communities network a good idea.
- Informal networks could be a mix of temporary or permanent – e.g. a young councillors network might be permanent and self running
- Protocol needed on recording meetings or not
- Greater clarity in e mails about who they've been sent to and what is their purpose
- Future of 109 may be affected by these developments and having a base at LGA would be good

nalc

Information

Quarterly summary report

National Association
of Local Councils

www.nalc.gov.uk

Published by
National Association of Local Councils (NALC)

109 Great Russell Street
London
WC1B 3LD

020 7637 1865
nalc@nalc.gov.uk
www.nalc.gov.uk

Every effort has been made to ensure that the contents of this publication are correct at the time of printing. NALC does not undertake any liability for any error or omission.

CONTENTS

INTRODUCTION

This report sets out progress delivering NALC's strategic plan including information on important internal issues, progress with our parliamentary and government affairs work, events, media coverage and publications and legal advice. The report will be largely work around the aims set out in the strategic plan and how we are working to achieve those aims. This report covers the period since the last report to Assembly in December – February.

CHIEF EXECUTIVE HIGHLIGHTS

- **NALC reflections -** The start of the new year begins a time for reflection, to consider what we have learnt from the last, most difficult year and consider future options. As part of my appraisal this year with Sue, Mike and Keith I was set five broad strategic objectives – to consider what the experience of the last year means for the way NALC works. Looking at the need for retaining 109, modernising our systems and developing staff capacity. To review and deliver a better, more responsive website which can meet members' needs and help provide key services. I was also asked to facilitate discussions about how the democratic oversight of NALC might develop as the success of remote meetings enable a different way of working for committees and the possible use of more informal networks. I am pleased to report that the Task and Finish Group has got off to a flying start with a real sense of consensus around how things needs to change. Relationships with county associations are key and improved though there are still risks associated with a wide range of capacities and resources. I was pleased to attend a session of the Isle of Wight Association to consider how it develops and I would commend their approach. Finally the importance of continuing to lobby government and others effectively and the success of our new campaign approach needs further development.
- **Civility in public life, working closely with SLCC -** An important piece of work over the coming months is to work closely with the SLCC and others to promote civility in public life including through the new code, lobbying for sanctions and developing a range of other support. This will require significant resource to deliver effectively.
- **Lobby day 2021** - Our remote lobby day went brilliantly and we will need to continue to press hard for the continuation of remote meetings where councils

want them. There has been much publicity around this and related matters over the last few weeks which has seen the sector have a much higher profile in the national and popular media which hopefully will help encourage more people from all ages and backgrounds to get involved and stand for election. Our Make a Change campaign is superb!

- **NALC governance elections -** We also need to keep an eye on NALC's own elections later in this year and you'll see from the agenda we are proposing some more informal councillor open days to encourage interaction between you all.
- And finally thanks to staff and colleagues in NALC and county associations for all the work they do, and the support of some really good councillors and please make sure councillors on your patch apply four our star councils awards here!! Good luck!

POLICY AND COMMUNICATIONS

This quarter's key headlines:

- **Engaging with government –** Through our annual Lobby Day, we promoted our priorities of remote meetings, local elections and funding, with county associations and NALC engaging through meetings and letters with over 130 Parliamentarians including ministers, shadow ministers and spokespeople. We hosted a meeting of the All-Party Parliamentary Group (APPG) on local democracy and held a Peers briefing. The final local government finance settlement for 2021/22 confirmed a successful outcome of our lobbying to ensure local councils are not subject to council tax referendum principles. Other advocacy included writing to the government about civility in public life and responding to consultations on the right to regenerate, model design code and local audit. Our plan for engaging with and influencing the new government is under continual review to ensure we raise the profile of the sector including in the devolution and recovery white paper.

- **Bills and legislation –** Worked with the APPG on Local Democracy (and Lord Lytton in particular) to ensure the Non-Domestic Rating (Public Lavatories) Bill Lords continued its passage through the House of Lords, Report Stage is due to take place 16 March followed by Royal Assent. Engaged with the Environment Bill, highlighting the role local councils are playing in tackling climate change and pressing for new powers and funding and met with officials in the Department for Environment, Food and Rural Affairs.

- **Campaigns -** A priority this quarter has been the Make a Change campaign with activities including securing media coverage, engaging with stakeholders and networks, organising online events and publishing further resources such as our Councillor stories videos. We also provided crisis communications support following the Handforth Parish Council video and assistance to Jackie Weaver. Our second survey of local councils on financial impact and recovery will be launched by the end of March.

- **Sharing good practice –** Published issue 1 for 2021 of LCR magazine, launched Star Councils 2020, held an In Conversation event aimed at larger councils featuring Biggleswade Town Council's work on strategic planning larger projects and a Make A Change event for the general public on becoming a councillor.

Next quarter's objectives:

- **Engaging with government –** Lobbying for extension of remote meetings, respond to publication of headline council tax statistics, Annual general meeting of APPG on local democracy.

- **Bills and legislation –** Environment Bill.

- **Campaigns –** Make A Change campaign, review policy positions regarding the creation of new councils.

- **Big themes –** Launch the dedicated webpage on young people, publish results and analysis of our climate change survey.

- **Sharing good practice -** Publish LCR magazine issue 2 of 2021, finalise our online events programme for 2021/22, judging for NALC Star Councils 2021.

MEMBER SERVICES

This quarters key headlines:

- **Coronavirus webpage** – we continue to provide regular updates on the Coronavirus webpage with email alerts to notify members of any changes.

These have included new guidance on preparing for face to face meetings and updates on the Government's roadmap out of lockdown

- **Legal queries –** High volume of legal queries and providing informal advices during COVID crisis period - as well as dealing with 246 written and telephone queries in December, January and February, the legal team provided 124 informal advices.
- **Legal updates –** A number of briefings were updated during this period: we reissued LTN 87 (procurement), LTN 31 (local council powers), LTN 13 (Policing your Area) and LTN 28 (Basic Charity Law)
- **Local Council Award Scheme accreditation –** 161 councils were accredited in 2020 across local and national panels. The first round of national panel accreditation for 2021 has received 22 applications. Which are will be assessed over March by our volunteer accreditation panellists
- **Local Council Award Scheme review of criteria –** a review of the criteria for the award scheme took place in 2021 and the new criteria for the scheme are now live for councils applying for the scheme in 2021. Updates included bringing the scheme up to date with new legislation eg website accessibility, as well as with new best practice eg an emphasis on customer service and on the environment.
- **Improvement and Development Board –** met in January and March and discussed a range of topics including CiLCA, Local Council Award Scheme, a new Masters in Public Leadership and Management, devolution, and much more
- **Working with County Officers –** fortnightly Zoom meetings have continued. NALC has also provided webinars for county officers on topics such as crisis communications and personal resilience
- **E-learning pilot –** Assessment of the pilot is taking place. Since the launch of our e-learning platform 286 individuals have registered for 492 courses. We are working with Breakthrough Communications to bring more courses tailored for local councils onto the e-learning platform.
- **Changes to the Member Services Team –** Charlotte Eisenhart, Head of Member Services begins maternity leave in March. Jane Moore will take on the role of Head of Member Services and Solicitor, and Anders Hanson joins the team as Projects Manager with specific focus on the Local Council Award Scheme, e-learning and website improvement.
- **Model Code of Conduct –** The LGA has launched their new model code of conduct for all tiers of local government. NALC has been in close contact with

the LGA throughout the development of this document. We are now a key stakeholder as the LGA develops additional guidance to support the implementation of the new model code of conduct.

Next quarters objectives:

- **COVID19 responsiveness –** We will continue to ensure a swift response to issues related to COVID19 and lockdown restrictions or changes
- **Website review –** We have started working with a user-testing company to help us assess the current website and how it is used. They will be reporting back in March/April with their learning and recommendations for next steps
- **E-learning –** Once the pilot assessment is complete we will be moving to commissioning new content that is specifically developed and tailored for town and parish councils

FINANCE AND ADMINISTRATION

This quarters key headlines:

- **Governance and remote meetings** –NALC governance continues to successfully operate remotely
- **Building management - 109** – we continue to ensure that 109 is well maintained during this period
- **LCAS-** we continue to successfully process new registrations onto the scheme and run meeting panels.
- **Events –** we successfully provide the administration support and process payments for numerous online events
- **Upgrade NALC email system** – we have successfully upgraded the NALC email system to provide greater capacity and reliability
- **E-learning –** working with Member services to assist with the rollout of the new e-learning platform
- **HR support -** ongoing provision of HR support to NALC staff including contracts to new staff members,

Next quarters objectives:

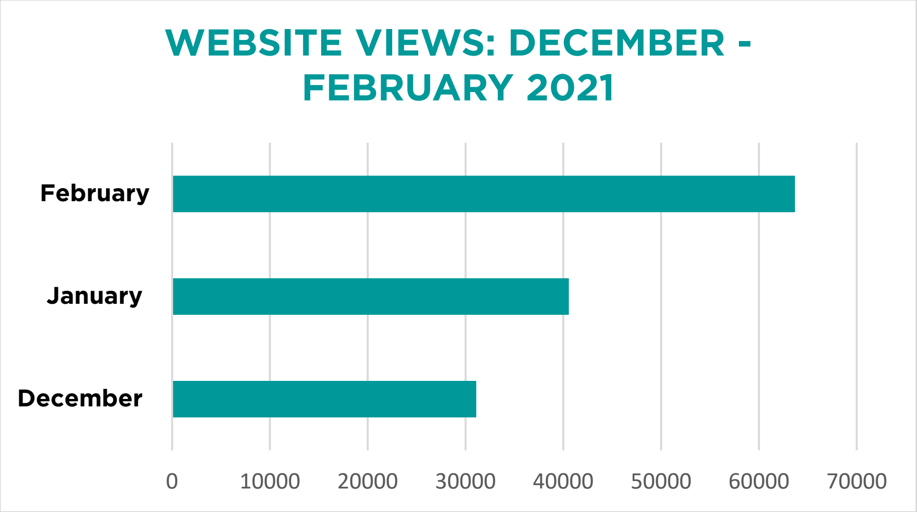
- **HR support** – rolling out 2021 staff appraisals to all NALC team and ensuring that all HR policies are up to date and compliant with HR legislation

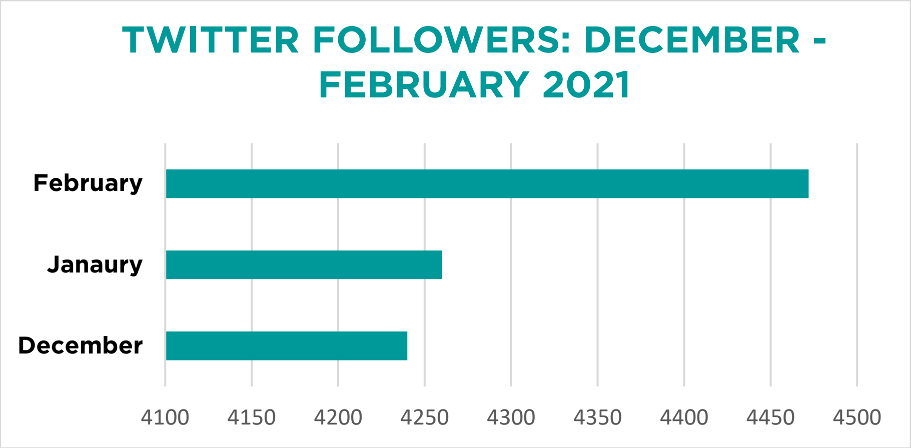
- **Policies and procedures -** ensuring all internal documents are up-to-date and easily accessible to NALC staff. Ensure that policies such as the NALC constitution, standing orders are up to date
- **Move to cloud based systems –** following the successful upgrade of the email system we are now planning for a move to the use of a cloud based system for all NALC system.
- **Support** – our service area provides support to Continue to work with other service areas to provide reliable support to our colleagues

KEY PERFORMANCE INDICATORS (KPI)

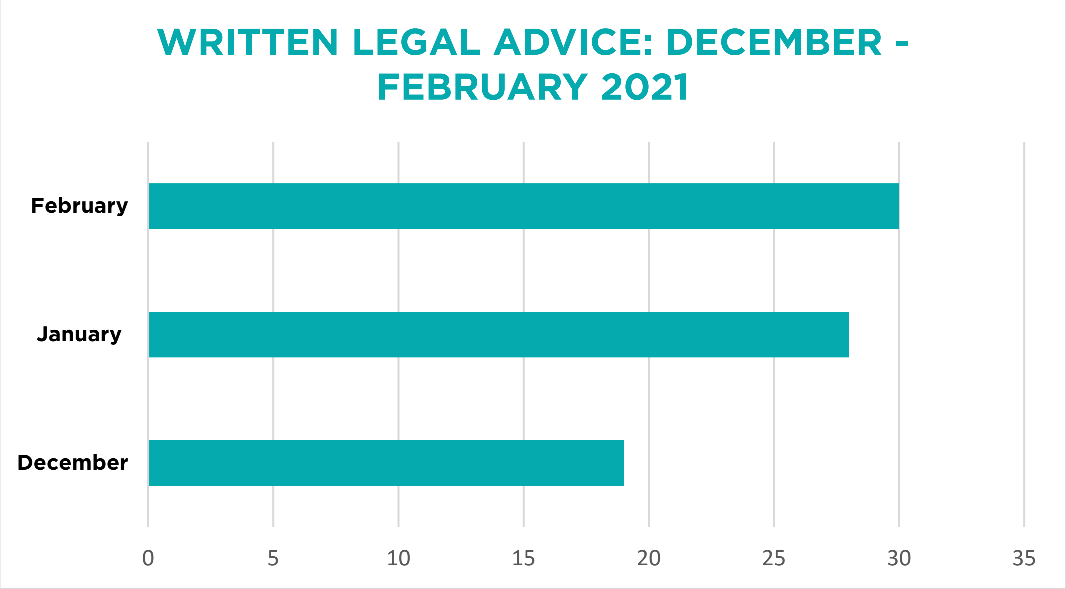
If you would like to see the full set of data, they are available on request.

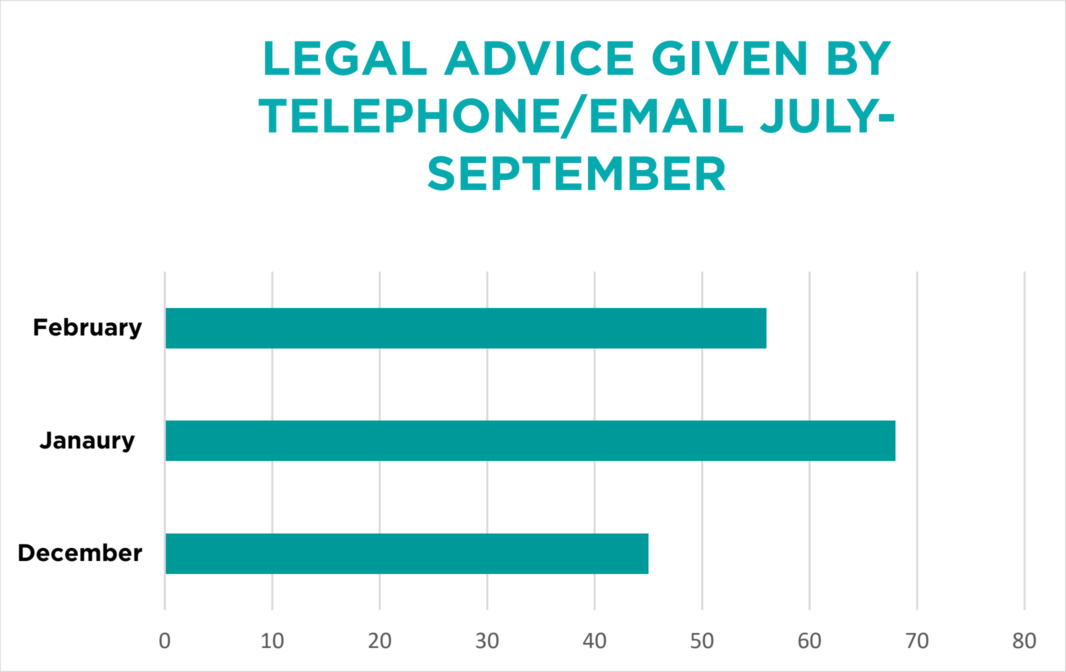
POLICY AND COMMUNICATIONS



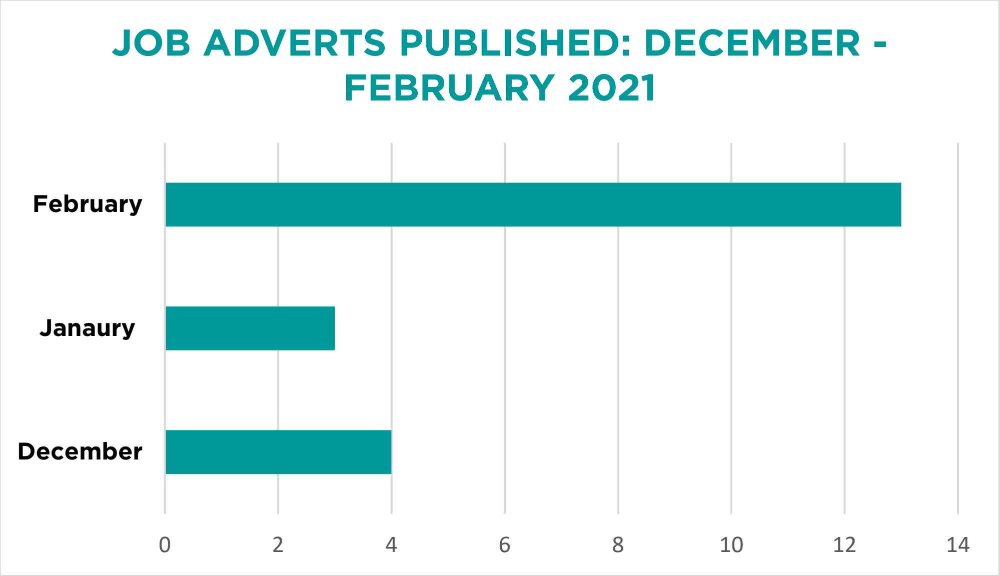


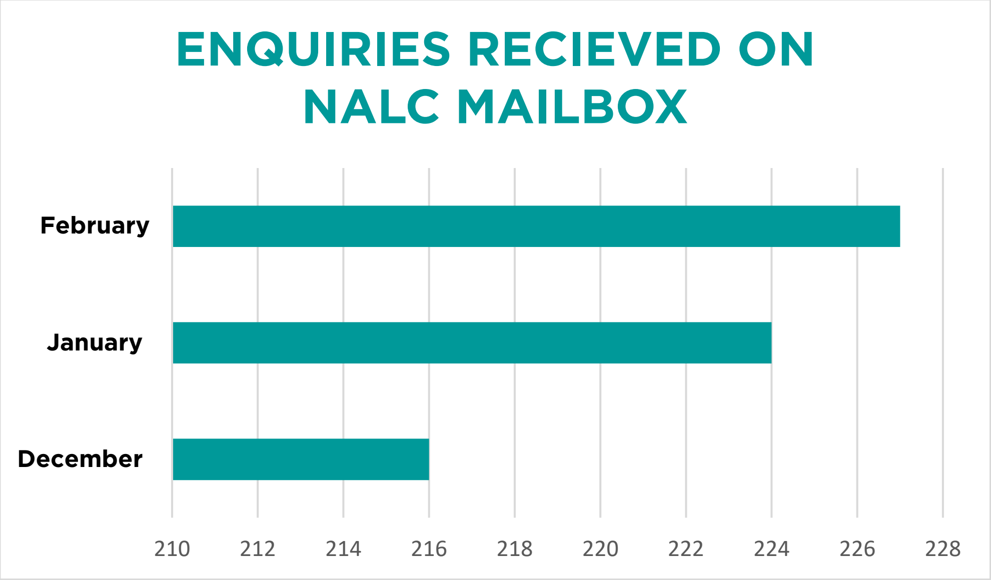
MEMBER SERVICES





FINANCE AND ADMINISTRATION





FURTHER INFORMATION

For more details and updates on NALC's activity, please read the chief executive's bulletin, which is circulated every Friday. If you are not subscribed to the bulletin, you can do so at www.nalc.gov.uk/newsletter.