# CITY OF WOLVERHAMPTON COUNCIL

# Scrutiny Board
## Minutes - 9 April 2019

## Attendance

### Members of the Scrutiny Board

Cllr Stephen Simkins (Chair)
Cllr Jasbir Jaspal
Cllr Peter O'Neill
Cllr Linda Leach
Cllr Philip Bateman MBE
Cllr Greg Brackenridge
Cllr Jasbinder Dehar
Cllr Dr Michael Hardacre
Cllr Sohail Khan
Cllr Martin Waite
Cllr Alan Bolshaw

---

# Part 1 – items open to the press and public

*Item No.      Title*

1      **Apologies for absence**
       Apologies for absence were received from Cllr Sweetman. Cllr Bolshaw attended as
       substitute.

       The Chair thanked officers for all of the work done throughout the last municipal year.

2      **Declarations of interest**
       There were no declarations of interest.

3      **Minutes of the previous meeting**
       Resolved:      That the minutes of the previous meeting be approved as a correct
       record and signed by the Chair.

4      **Minutes of the WMCA Overview and Scrutiny Committee 25 February 2019**
       The Board considered the minutes of the West Midlands Combined Authority
       Overview and Scrutiny Committee meeting held on 25 February 2019.

       Concern was expressed that the meeting was not quorate and that this could indicate
       that scrutiny was not being taken seriously.

       The Chair stated that it was due to how the legislation was written and that steps
       were being taken to try and address the problems through the governance
       procedures. The Chair stated that it was hoped that in the future the WMCA O&SC
       would start to bring updates back to each constituent authority.

The Board queried how many times the meetings were inquorate, and it was stated that this happened quite regularly but that turnout was better in the working groups.

The Board considered that it should be noted that these bodies are deemed important and that if they are constituted in such a way that there are issues such as being inquorate, then these issues needed to be addressed. Public money was going into these groups and it needed to be used productively. A board member stated that he had been involved in county wide organisations for a long time and that they had ended because they were not accountable, and it seemed probable that not many members of the public would know what the WMCA was or what it did.

It was agreed that concerns about governance arrangements needed to be fed back to the WMCA O&S Committee.

The Chair noted that there were only two Scrutiny Officers for the WMCA O&SC and that other councils including Wolverhampton were often asked to help with the administration of meetings.

The Board also noted that to amend the quorum of the WMCAO&SC would require intervention from central government as it could not be done locally.

Resolved:     That concerns regarding the governance arrangements of the WMCA O&S be fed back.

5     **Matters arising**
There were no matters arising.

6     **The Call-In Process and Overview and Scrutiny Procedure Rules**
The Board considered the recent call-in and the processes that were currently in place for dealing with call-ins.

The Board considered that the procedure rules needed to be looked at and that in the future a reason for the call-in had to be specified.

The Board also considered that clarification was required around the exclusion of the press and public from meetings.

Resolved:     That a scrutiny working group be convened to consider the call-in procedure.

7     **Cyber Security**

The Board welcomed Gail Rider, Head of ICT to the meeting.

The Director of Governance who was the Senior Information Risk Owner (SIRO) had recommended a report be presented to Scrutiny Board to provide an overview and understanding of how Cyber security was managed within the authority. The report included information on the robustness of processes and preventative measures that were in place, an overview of the authorities' cloud storage approach and the on-

going roadmap that assured constant and up to date approaches to new threats and challenges.

It was stated that the Council was a Microsoft partner which meant that any processes were supportive and progressive.

The Council adopted a cloud first approach, but this wasn't always an option as some applications were not be cloud ready. The cloud was provided by Microsoft, which was one of the most secure and the Council only paid for what it used. There was a secondary data centre in Stafford and a proportion of what the Council run was replicated there.

The Council took a very preventative approach to cyber security and it was stated that there had been four attempted attacks since Christmas, all of which had been stopped.

It was confirmed that the Council did apply patches regularly and was continuously updating firewalls and antivirus software whilst also working closely with partners including the Information Governance team.

The Council's cyber security had been assessed and once deemed to be one of the safest in the region.

The Board queried the use of multiple and often very complex passwords and it was confirmed that the Council's password policy was currently under review and that the team were aware that it could not be overly secure as this might make it harder for people to use the services on offer.

The Board considered the issue of the phishing campaigns that had been carried out by Information Governance. The first had been carried out in October 2017 with 608 emails being opened and 500 employees attempting to click on link. The more recent exercise had resulted in 93% of emails not being opened and only 4% attempted to click on the link.

The question was raised as to what were the big-ticket issues that could really cause problems if we got them wrong such as a sustained denial of service attack (if services went down for a long time), the safeguarding of data or problems with the urban traffic control centre for the black country including the threat of hostile actors trying to take it down.

It was stated that the Council was looking at every single service it had and every application including where it sat, how it was backed up and how it was secured. The Head of ICT stated that she had managed to obtain match funding to put in additional controls. The Head of ICT stated that in relation to the Urban Traffic Control System she would expect that this was replicated in Stafford with the servers based here.

It was noted that the Urban Traffic Control System worked off a mobile network and the question was raised as to whether this could be interfered with. The Head of ICT stated that she would investigate this and provide a response later.

The Board raised the issue of interfering with as well as stealing data. Data sharing was becoming more important, with organisations such as the Fire Authority working

with the police and possible funding from the government being provided to create a data hub.

Also, of concern were areas such as the linking of internet-based devises such as when your doorbell rang and can you could see who was there on your phone. The concern focused around the fact that security had not always been built into the systems within the systems.

The Board considered flood risk defences and whether they could provide a backdoor into higher level systems. It was thought that the Council needed to be aware of where it set the levels of what was allowed on everything and that nothing should be allowed onto the network until the Council were certain that it was as safe as it could be.

The Board queried how the Council monitored the people that had access to information and how it would manage a disgruntled employee with access to sensitive data.

The Head of ICT stated that the Council had to have trust in employees but that where a department was perhaps going through a restructure certain rights may be removed from certain individuals if there was deemed to be a risk.

The Board considered what the cost to the Council would be if there was a major cyber attack including all the legal implications linked to breaches of data protection regulations.

The Board considered that as councillors, they were all now responsible for the data they held and that they needed to be more focused on the issues.

The Board queried how cyber security linked into emergency planning and resilience. It was stated that the Council's ICT team worked very closely with the Emergency Planning and Resilience Team and that the work currently being undertaken would produce a report highlighting any gaps and options for fixing them.

The Head of Governance stated that every service in the Council had a business continuity plan and that turnaround times had been identified with the resilience team. Levels of priority had also been identified and had all been refreshed in the last month.

The Board considered that as councillors, they took on a lot of case work and the this made them data controllers and responsible for the data they held on residents. It was noted that everyone had different ways of dealing with this data and different hardware with different levels of security and it as queried whether a cloud-based solution could be put in place for councillor casework.

The Head of ICT stated that any casework carried out on Council supplied equipment would be secure and that she could investigate the possibility of a home devise and cloud storage.

The Board also sought information on data sharing as some people might be doing things that were not safe without realising that they were not safe. It was recommended that this be brought back to a future meeting.

The issue was raised that the majority of breaches were not caused by people disobeying the rules on purpose but by human carelessness, connecting the wrong things to the wrong thing etc. The recommendation was made that the cyber security training and monitoring of who had done the training be looked at to perhaps restrict access to the Council network to those who had not recently completed the training.

It was also recommended that an item on cyber security be added to the work plan for the next year.

**Resolved:** (1) That an item on cyber security be added to the scrutiny work programme;

(2) That the Head of ICT investigate the possibility of linking mandatory cyber security training with access to the Council's networks;

(3) That the Head of ICT investigate the possibility of a cloud-based solution for councillor casework;

(4) That the Head of ICT investigate the matter of the Urban Traffic Control System and the risks associated with it.


8 **Work programme**
The Board received a verbal update from Cllr Ahmed on the work of the Scrutiny Review into Youth Violent Crime. The next meeting of the Review group was 20 June 2019 when the matter of exclusions would be considered.

Resolved: That the workplan be agreed.


9 **Forward Plan(s)**
Resolved: That the Forward Plans be noted.

10 **Annual Scrutiny Planning Event**
Resolved: That any recommendations be brought back to a future meeting.