Audit, Risk & Assurance Committee

Date	4 March 2021
Report title	Update on Cyber Security & ICT processes
Report Author	Jason Danbury Strategic Head of Digital and Data Email: Jason.Danbury@wmca.org.uk

Recommendation(s) for action or decision:

The Audit, Risk & Assurance Committee is recommended to:

(1) Note the use of the *Protection of Digital and Data Systems and Information - Acceptable Use Policy* (AUP) to provide support to the organisation.

1.   Purpose

To provide an update on cyber security and ICT processes.

2.   Background

The maturity of WMCA's Information Assurance is an ongoing process that incorporates national frameworks and best practices such as the HMG Security Policy Framework and National Security Centre guidance.

Confidentiality, Integrity and Availability (CIA) of data underpins Information Assurance and Information Security Management, with Cyber Security and its processes forming a sub-set of this subject. To support the organisation and help individuals to better understand areas of personal accountability a *Protection of Digital and Data Systems and Information - Acceptable Use Policy* (AUP) has been created and sets out 5 main categories for awareness.

The AUP is particularly important in the current climate given the necessity of remote and home working. The 5 categories set out in the AUP are:

1) Protection

    A general reminder of good practices in protecting individuals and the organisation. Setting out processes to adhere to and what to do if experiencing problems.

2) Working Remotely

    The Covid-19 pandemic has resulted in a significant shift in working practices with a reliance on remote working. The AUP provides guidance on how best to work outside of the traditional work environment.

3) Personal Use of WMCA IT

    With the blurring of lines between work and homelife during the current situation, the AUP helps provide clarity regards the use of WMCA equipment.

4) Storage

    Providing guidance on the transportation and storage of physical and digital information is an important part of maintaining confidentiality and integrity.

5) Loss or Compromise

    The AUP provides clarity on what to do in the event of WMCA information or systems being lost or compromised.

All individuals requiring access to WMCA systems will need to have signed up to the *Protection of Digital and Data Systems and Information - Acceptable Use Policy* (AUP) and in doing so, understand the personal accountability of their actions and activities.

The above, supplements the cyber security processes and systems that are already in place and a further update relating to this area will be given in the confidential part of the agenda.

3.   Financial Implications

There are no Financial Implications directly associated with this paper.

4.   Legal Implications

There are no Legal Implications directly associated with this paper.

5.   Equalities Implications

There are no Equalities Implications directly associated with this paper.

6.   Inclusive Growth Implications

There are no Inclusive Growth Implications directly associated with this paper.

7.   Geographical Area of Report's Implications

There are no Geographical Area of Reports Implications directly associated with this paper.

8.   Other Implications

The reliance upon remote working has accelerated the organisations use of technology and the associated skills. Additional support is required for some staff to enhance their experience and their understanding of how best to use the required IT systems.

9.   Schedule of Background Papers

Information Assurance and Information Security Management Policies and Procedures