

STAFFORDSHIRE MOORLANDS DISTRICT COUNCIL

Resources Overview & Scrutiny Panel

25 November 2020

TITLE:	Information Governance Update
PORTFOLIO HOLDER:	Councillor Tony Hall - Portfolio Holder for Customer Services
CONTACT OFFICER:	Vanessa Higgins - Information Business Partner
WARDS INVOLVED:	All

1. Reason for the Report

- 1.1 To provide an Information Governance update which details how the Council continues to embed good information management practices through its ASSURED framework.

2. Recommendation

- 2.1 That the Panel notes the contents of this update.

3. Executive Summary

- 3.1 Good information management practices are the responsibility of everyone within the Council. To promote these good practices and to oversee the Council's approach to good information governance is the role of the Information Governance Group (IGG).
- 3.2 The Council has developed a suite of policies and guidance documents as part of its ASSURED framework, which are accessible to all employees and councillors through the [intranet](#).
- 3.3 The Council has made significant progress in its approach to information governance including the use of asset registers, impact assessments, breach reporting, and an ongoing action plan that ensures training is at the heart of this approach.

4. How this report links to Corporate Priorities

4.1 Information Governance contributes to Aim Two of the Corporate Plan – *to use resources effectively and provide value for money.*

5. **Alternative Options**

5.1 This report is for information only and no decision is required.

Mark Trillo

Executive Director (People) and Monitoring Officer

Web Links and Background Papers

Information Governance Action Plan
Information Governance Group papers
ASSURED framework policies

Contact details

Vanessa Higgins
Information Business Partner
vanessa.higgins@highpeak.gov.uk

6. **ASSURED in our approach**

6.1 The Council's approach to good information management is encapsulated in the word ASSURED, which refers to the desired lifecycle of data within the organisation (**A**lliance, **S**ources, **S**tores, **U**ses, **R**etains, **E**rases, **D**ata). The council has developed a suite of policies and guidance documents as part of its ASSURED framework, which are accessible to all employees and councillors through the [intranet](#) page of the same name and includes:

- Data Protection Policy
- Document Retention Schedule
- ICT Use and Information Security Policy
- Councillor ICT Equipment and Information Security Agreement
- Email Guidance
- Information Protective Marking Guidance
- Data Breach Reporting Portal



6.2 A review programme is in place for each of the Council's key information governance related policies. In 2020 the ICT Use and Information Security Policy was reviewed and is in the process of being rolled out to all employees via the Council's online training platform, Alliance e-ssentials. Next year will see the document retention schedule and information governance policy reviewed and refreshed.

7. **Information Governance**

7.1 Good information management practices are the responsibility of everyone within the Council. To promote these good practices and to oversee the Council's approach to good information governance is the role of the Information Governance Group (IGG). The group was first formed in 2015 and is led by the

Senior Information Risk Officer – Executive Director (People) & Monitoring Officer – supported by the Information Business Partner and focuses on:

- Policy development and dissemination
- Compliance monitoring and assurance against the Council's policy
- The need to ensure good information governance compliance by third parties working with the Council
- Improving efficiency in the use of technology
- The technology and infrastructure to support good information governance

7.2 The IGG meets quarterly and considers set items such as data breaches, data protection impact assessments, information asset registers and progress against the information governance action plan at each meeting:

- Data breaches: the council developed a new automated breach reporting portal, similar to the complaints portal, earlier this year. This enables potential breaches, however small, to be logged via the intranet or website. All breaches are considered by the Data Protection Officer in the first instance before being reported to the IGG, and the ICO if required. Improvements to processes and additional training, if needed, are put in place to reduce further risks of breaches occurring.
- Data Protection Impact Assessments (DPIAs): every project entered into by the Council and managed through the Transformation Board has to complete a stage one DPIA to assess the potential impacts of the project on personal data. If required, the project then proceeds to a stage two DPIA, with risk mitigation action required and regular updates back to the IGG.
- Information Asset Registers (IARs): during 2019 the Council made considerable progress in developing a suite of IARs across all of its service areas, which map out the key data assets used by the service. These are comprehensive registers which have a central role in the ASSURED framework in helping to ensure that data is sourced legitimately, stored safely, used correctly, retained for a limited period, and erased when no longer required. The IGG oversees a programme of challenge sessions whereby Heads of Service present their IARs to a critical friend challenge by the group to ensure the data practices within the service meet the standards required by the council.
- Information Governance Action Plan: the council has made good progress against the action plan, the main areas of focus now being a review of Privacy Notices; ongoing and bespoke training; preparing for the EU transition and its impact for GDPR; and 3rd party data assurance. Some of the Council's more recently completed projects are outlined below.

8. Information Protective Marking

8.1 The Council worked with its strategic risk partner, Zurich, in 2018 to develop an approach to protectively marking documents and information being shared internally with colleagues and externally with partners. An information guide

was produced and rolled out to all employees through Alliance e-ssentials with face to face training sessions for teams handling bulk personal data.

- 8.2 The move to Microsoft 365 will bring additional protective marking and data protection benefits, as the improved functionality will allow greater control over data protection and retention policies within the platform itself.

9. **Privacy Notices**

- 9.1 As part of the GDPR preparations, the Council ensured that it had a comprehensive privacy notice on the website as well as tailored notices within individual service areas where this was required.

- 9.2 Since then we have also created specific pages on the website for councillor privacy notices that include all aspects of the member role. In the last 12 months we have also developed an animated privacy notice deployed through the [website](#) to give users an immediate, visual message about why and how their data is used when accessing our services.

10. **Training**

- 10.1 Relevant training for employees and councillors on information management is key to the success of the Council's approach. In the run up to GDPR implementation a programme of externally facilitated training was devised and delivered.

- 10.2 This has been followed up by largely in-house tailored training linked to new developments and new working practices such as revisions to the ICT Use and Information Security Policy, Protective Marking, team specific training and councillor data protection training as part of the induction programme following last year's elections. Maintaining a programme of information governance related training will remain one of the IGG's continuing actions.