Item 15

North York Moors National Park Authority

1 October 2018

GDPR Update

1. **Purpose of the Report**

1.1 To update Members on work completed and currently being carried out to comply with the General Data Protection Regulations.

2. **Background**

2.1 At the NPA in September 2017, Members were given background information and outline plan regarding the Authority's approach to preparing for the implantation of the EU General Data Protection Regulation which came into force in the UK in May 2018. As Members will be aware, the Authority was previously subject to the terms of the Data Protection Act 1998 which controlled how personal information is used by organisations.

2.2 The original Act enshrined 'data protection principles':

1. **Lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. **Purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy** - Personal data shall be accurate and, where necessary, kept up to date.

5. **Storage limitation** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. **Integrity and confidentiality** - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.3. These remain unchanged under GDPR, but there are a number of additional responsibilities for organisations including;

- Individuals must opt-in whenever data is collected and there must be clear privacy notices. Those notices must be concise and transparent and consent must be able to be withdrawn at any time;
- An individual will have the 'right to erasure' with all information being permanently deleted;

- Protection Impact Assessments (PIA) are mandatory and must be carried out when implementing new systems/processes. A PIA helps an organisation to ensure they meet individuals' expectation of privacy
- Organisations must be able to demonstrate they comply with the GDPR's principles. Mandatory activities to demonstrate compliance include:

    - Staff training
    - Internal audits of data processing activities
    - Availability of 'expertise' via the Data Protection Officer
    - Implementation of Protection Impact Assessments

3 Pre-GDRP Deadline Work

3.1 Prior to the end of May a small team of NYMNPA Officers have worked closely under the guidance of the Data Protection Officer from Scarborough Borough Council to prepare the Authority for the transition to the new regulations. A brief outline of the work carried out is below:-

- Established what Personal Data (PD) the Authority held using a simple data survey.
- Examined all processes that involved PD and recorded these in a PD Asset inventory.
- Mapping of key complex processes to better understand where the PD travelled along the process.
- Cleansed existing PD that we had no justification to keep, couldn't prove its accuracy or hadn't obtained the correct consent.
- Completion and publication of a new Privacy Statement.
- Completion of new Data Protection Policy.
- Completion of Data Protection Impact Assessment spreadsheet to be used for any new process or system going forward.
- Completion of GDPR specific risk register.
- Reviewed existing consent forms, both electronic and paper to ensure compliance.
- Attended departmental meetings to raise awareness.
- Ensured that all staff completed GDPR online training.
- Confirmation that the Authority's Data protection Officer would be provided by Scarborough Borough Council via the existing Legal Services Agreement.

4 Post GDPR Deadline Work

4.1 Work on GDPR hasn't stopped since the deadline passed as the Authority should now ensure ongoing GDPR compliance. This involves the ongoing education of Officers and testing of systems and processes to ensure they are secure along with managing the GDPR specific risks and mitigating these where possible.

4.2 There was a concern that people might use GDPR to "spam" Authorities with Subject Access Requests (SARs) in a similar way as FOIs are used. Thankfully this hasn't been the case and so far we have only had one SAR, which was dealt with well within the required timescales.

4.3 The GDPR team have continued to provide advice to Officers around breach notification, wording of consent forms and new process management..

4.4 Whilst Officers intend continuing to use SBC's Data Protection Officer as our point of contact for more complex data protection issues, the Authority will need to maintain a good level of understanding and knowledge of data protection so we can carry out day to day function.

5. **Legal Implications**

5.1 There are no legal implications arising from this report.

6. **Recommendation**

6.1 That Members note the work that has been carried out and that there is an ongoing need to ensure compliance with GDPR.

Contact Officer:
Simon Baum
ICT Manager
01439 772700