Digital Innovation & Efficiency Committee

Item No.

Report title:	**General Data Protection Regulation**
Date of meeting:	**11 May 2018**
Responsible Chief Officer:	**Geoff Connell Head of IMT and Data Protection Officer**

Strategic impact

This report provides the Committee with information on the progress of the Council's preparations for the implementation of the General Data Protection Regulation on 25th May 2018.

Executive summary

The report sets out the progress on the preparations for the implementation of the General Data Protection Regulations (GDPR)

Recommendation: to note the progress on the preparations for the GDPR

1. Purpose of the report

1.1 This report sets out the progress on the preparations for the implementation of the General Data Protection Regulations.

1.2 The report is for information.

2. Background

2.1 The GDPR will be implemented on 25th May 2018.

2.2 NCC has produced a project plan for the GDPR and this report sets out the progress made against the plan.

2.3 The Information Compliance Group (ICG) has considered and discussed the project plan and a GDPR Business Leads Working Group (BLWG) has also been set up to take the plan forward. The business leads have ensured that work required under the project plan is undertaken by the services as necessary.

2.4 The following work streams have been prioritised by the ICG and BLWG

- New consent rules and privacy notices
- Changes regarding data controllers and data processors
- Privacy by Design and Data Protection Impact Assessments (DPIAs)
- Security Breaches
- Record of Processing Activity (ROPA)
- Training
- Communications

2.5 Although there is a considerable amount of work to be done to ensure that the County Council is fully compliant with the GDPR, it should be noted that the Council was in a good position to meet many of the data protection requirements because of the work that was undertaken to prepare the Council for the Information Commissioner Office's audit of the County Council in October 2016.

2.6 Further details of each work stream are set out below.

3. New Consent Rules and Privacy Notices

3.1 The GDPR contains stringent new conditions on data controllers to obtain valid consent from data subjects.

3.2 The GDPR says that consent must be freely given, based on a real choice and without conditions. If someone cannot access a service without the Council collecting and processing their information, or if we ask for their consent but would actually process the information anyway even without their permission, then neither of these meet the criteria and would not be considered as true consent. This means that from 25 May 2018 we will move away from asking for consent and our work will mostly be based on our published privacy notices.

3.3 A privacy notice is how we tell people what we will do with their data. As a large Council providing a wide range of services, one privacy notice will not be enough to cover everything that we do so we will have a layered approach with separate notices for services and the work that they do. What this means in practice is that when we begin talking to someone about providing a service or some help, we will tell them at the beginning what we will do with their information.

3.4 All our privacy notices are currently being reviewed. At the moment our main focus is on the services processing large amounts of sensitive personal data. This means Children's Services and Adult Social Care, Trading Standards, Blue Badge applications and Youth Development in Norfolk Fire and Rescue Service. The remaining services will then be addressed.

3.5 New privacy notices will be available on our website from 25th May 2198 and will be provided on paper for people who do not have internet access.

4. Changes regarding data controllers and data processors

4.1 The GDPR requires data controllers to obtain sufficient guarantees from data processors and imposes direct obligations and liability on data processors for the first time. This means that we are amending all our contracts with service providers who act

as our data processor to reflect these more rigorous requirements.

4.2 Procurement has reviewed all these contracts and is in the process of sending out amendments to the terms and conditions of these contract. Their focus is on contracts involving the processing of large amounts of sensitive personal data. The remaining contracts will then be addressed.

5. Privacy by Design and Data Protection Impact Assessments (DPIAs)

5.1 The GDPR requires data controllers to introduce data protection by design and data protection by default at the time of the determination of the means for processing and thereafter.

5.2 The GDPR also requires the completion of DPIAs in respect of processing that is likely to result in "high risk" to the rights and freedoms of data subjects and that the Information Commissioner's Office should be consulted in respect of any high risks that cannot be mitigated.

5.3 This means that any proposed projects/services/other processing activities involving high-risk processing of personal data must consider the privacy risks before implemented and mitigate these risks. This can best be done by undertaking a DPIA before any firm decisions are taken regarding the proposal.

5.4 The GDPR also requires data controllers to consult with the Information Commissioner's Office (ICO) if any high risks cannot be mitigated.

5.5 We have revised the County Council's procedures to reflect this and training will be provided to all relevant staff in early June on how to undertake a DPIA.

6. Security Breaches

6.1 The GDPR requires data controllers to report breaches to the ICO without undue delay and where feasible within 72 hours of having become aware of it. All personal data breaches must be documented by data controllers to enable the ICO to verify compliance.

6.2 The data controller must also notify individuals affected by the breach in clear and plain language where the breach is likely to result in a high risk to the rights and freedoms of individuals.

6.3 We have revised the County Council's procedures to reflect this and currently piloting the procedures with relevant officers.

7. Record of Processing Activity (ROPA)

7.1 The GDPR requires the data controller to maintain records of all processing activities as data controller and data processor.

7.2 Work is well underway in producing a ROPA but this is a considerable task so the focus

has been on services processing of large amounts of sensitive personal data. The remaining services will then be addressed.

8. Training on the GDPR

8.1 The mandatory e-learning for GDPR was introduced in March for all staff and members. This means that all new staff and members and those staff and members who are required to undertake the two-year refresh training will complete the new course.

8.2 All remaining staff and members can undertake this training on a voluntary basis before they are required to do so under the mandatory two-year refresh training.

8.3 Training will be arranged for members and will also be offered to staff on privacy notices/consents as required.

9. Communications

9.1 A communications plan has been produced to ensure that staff are aware of the changes and kept informed on the progress of the work described above. This includes six articles in Friday Takeaway; Norfolk Manager; departmental newsletters; and references in SMT blogs.

9.2 The public will also be informed about the changes in Your Norfolk; Your Norfolk Extra; and on the Council's web site.

10. Financial Implications

10.1 There are no decisions arising from this report. Most of the work has been undertaken by services' existing resources but an additional £150k has been set aside to assist with work associated with the GDPR both before and after implementation.

11. Issues, Risks and Innovations

11.1 The GDPR provides for the imposition of substantial fines for failure to comply with the Regulation. But the Information Commissioner has confirmed that the ICO's proportionate and pragmatic approach will continue after 25th May so that enforcement and fines will be a last resort. Although not all the preparations will be fully complete by the 25th May, work will continue with all the services to ensure that the Council is fully compliant, based on a risk assessed and prioritised forward plan of activity.

Officer Contact

If you have any questions about matters contained in this paper, please get in touch with:

Officer name:	**Geoff Connell**	**Tel No.:**	**01603 222700**
	Pamela Cary	**Tel no.**	**01603 222449**
Email address:	**geoff.connell@norfolk.gov.uk**		
	pamela.cary@norfolk.gov.uk		

IN TRAN
communication for all

If you need this report in large print, audio, braille, alternative format or in a different language please contact 0344 800 8020 or 0344 800 8011 (textphone) and we will do our best to help.