HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Data Protection Compliance: Update on Action Plan
Meeting/Date:	Corporate Governance Committee – 24th March 2021
Executive Portfolio:	Executive Councilor for Digital and Customer
Report by:	Information Governance Manager & Data Protection Officer
Ward(s) affected	All Ward(s)

EXECUTIVE SUMMARY:

The Information Governance Service for Huntingdonshire District Council (HDC) is currently provided by 3C ICT Shared Service hosted by Huntingdonshire District Council. This also serves South Cambridgeshire District Council and Cambridge City Council.

The Information Governance (IG) Team lead on Information Requests, Data Protection Compliance, Data Privacy and provide additional advice around Information Management. The team is headed up by the Information Governance Manager who is also the Data Protection Officer.

The IG Team is a fairly new team formed in 2020. Due to this, the IG team carried out a review of the Data Protection arrangements in June 2020 to determine the areas for priority action.

This report provides a status update on the suggested actions identified as part of the review.

Recommendation(s):

Corporate Governance Committee is asked to note the contents of this report.

1. PURPOSE

1.1 The purpose of this report is to provide a status update on the actions identified as part of the Data Protection gap analysis (review).

2. SCOPE

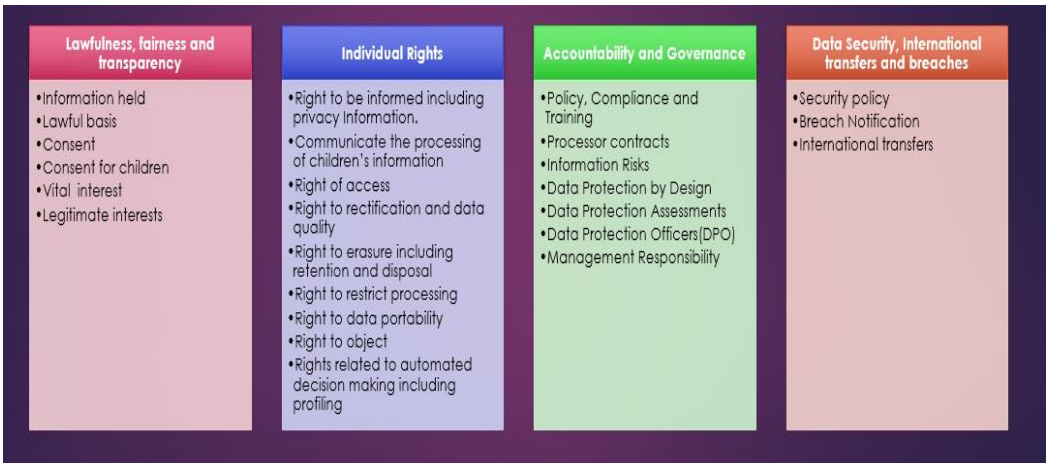
2.1 The Gap Analysis was undertaken in June 2020.

2.2 The purpose of this was to determine the which areas needed to be focused on in order to ensure Data Protection Compliance.

2.3 The main areas covered included: Lawfulness, Fairness and Transparency, Individual Rights, Accountability and Governance, Data Security, International Transfer and Breaches.

2.4 Each area consisted of a number of sub-categories.

The scope for each category is provided below:



3. FINDINGS / ACTIONS

3.1 The overall finding from the review was that, whilst appropriate procedures were generally in place, these were generally informal, incomplete, and/or inconsistently applied

3.2 Improvements were required in the following areas:

Area	High Level Finding	Risk	Actions needed	Status	Due Date
Information Asset Registers / Flows/ Records of Processing (Article 30)	Although some Information Asset records were held by Service areas; we do not hold a central repository.	The risk here is that there is no overview of our processes / systems which could result in delays to information requests; inappropriate controls being in place; no clear view on dependencies in terms of ICT systems when a change is made; etc.	Create a central information asset register. Review of existing information to ensure this is up to date, it includes transfers of information and safeguards in place.	**In progress.** IG team have started compiling a central list of information assets.	End of May 2021
Records of Processing (Article 30)	Although the Information Asset Register does collect most of the information required for Article 30; this is not held centrally; in addition to this, more information would be required on disclosures and	There is a risk that information is inappropriately being transferred (i.e. there may not be appropriate adequacy arrangements or appropriate technical safeguards in place)	Review existing information to ensure transfers are documented. Incorporate this within the central Information Asset Register	**In progress**. As above.	End of May 2021

Area	High Level Finding	Risk	Actions needed	Status	Due Date
	transfers.				
Policies	Although there are some policies accessible on the Council's intranet pages, a number of these are out of date. To add to this, there are also additional IT Policies located within a repository (Protocol Policy) which is not accessible to all staff as they are not published on the Intranet.	The risk is that staff are not aware of their obligations and therefore put the Council resources at risk.	Policies need to be reviewed and published as appropriate.	**In progress.** Gap Analysis of Information Governance Policies has been undertaken to establish what is published and what needs to be drafted**.** **Detailed Plan yet to be established of when policies are to be reviewed and updated. (Update to be provided at June 2021)** IT Policies have started to be reviewed by ICT. ICT Acceptable Use Policy was circulated on behalf of 3C ICT to the Information Governance Group Members on 5/02/2021 for comments. **Further revisions are however required.**	End of June 2021

Area	High Level Finding	Risk	Actions needed	Status	Due Date
Training Arrangements	The requirement by the ICO is that training is undertaken at least every two years. New starters are required to undertake e-learning as part of their induction process. For many existing staff, e-learning was undertaken in preparation for GDPR in 2018. This therefore means a number of staff will be coming up to the 2-year threshold for retraining. To date, there has been limited communication to	Although not in breach of the Act, by undertaking training every 2 years, this frequency is not in line with other partners in the public sector (e.g. NHS). This therefore creates a hurdle when signing up to Information Sharing Agreements. Without undertaking training staff will not be aware of what they should or should not do.	Need to review Information Governance training provision including content; reporting and frequency for undertaking training. The requirement for refresher training will need to be reinforced.	**In progress** Content for new Learning Management System (LMS) has been reviewed. Suggested training modules to be rolled out have been communicated with HR. Frequency has also been discussed with HR as part of review of training needs analysis**.** **HR to determine when the new modules will be ready to roll out (as this is part of a wider implementation)**	End of May 2021

Area	High Level Finding	Risk	Actions needed	Status	Due Date
	enforce the requirement for refresher training for existing staff.				
Information Sharing Arrangements	Although there are Information Sharing Agreements in place across the Council, there is no central register for this. There is no clear visibility if there are appropriate contracts / sharing agreements in place.	If a contract is not in place where data is being processed on behalf of the Council by a Data Processor; this is likely to be a breach of GDPR.	An Information Sharing Log needs to be created. The Information Asset Register work (identified above) is also likely to identify where Contracts are needed.	**In progress.** The IG team have started collating Information Sharing Agreements as of when they become aware of them. There has however not been an amnesty to identify ones already in place. **Email is scheduled to go out to Service areas requesting copies of Information Sharing Agreements in place**	End of May 2021
Incorporation of Privacy by Design in Projects	Data Privacy Impact Assessment (DPIAs) are	DPIAs may not be completed and therefore privacy risks may either not	The DPIA process and document to be reviewed and	DPIAs are taking place. The form needs to be reviewed and aligned to	End of June 2021

Area	High Level Finding	Risk	Actions needed	Status	Due Date
	completed; but it is unclear if this is always the case. DPIAs are currently treated as standalone documents to be completed at project initiation. Not all changes, go through a standard project process.	be identified / identified in a timely manner.	communicated. Its requirement needs to be better communicated and/or integrated with Project / Change processes.	other project / compliance processes. **Review of process / form not started.**	

4 LOOKING FORWARD

4.1 Ensuring ongoing compliance with Data Protection Legislation (DPA 2018 and GDPR) has been the focus of the Information Governance team.

4.2 The Information Governance team will continue to work with Service areas to address gaps identified as part of the Gap Analysis undertaken (on Data Protection Compliance) and provide updates during the Information Governance Group meetings.

5. KEY IMPACTS/RISKS

5.1 The key impact of non-compliance with the Data Protection legislation along with GDPR is public scrutiny from the regulator.

5.2 Poor service or inadequate information management will lead to loss of trust from our customers. Inability to act in accordance with the Act and the Governments accountability and transparency directive will lead to reputational damage.

5.3 Furthermore, the right of access is bound with the Human Rights Act in respect of the right to privacy. Unlawful disclosure of personal information may lead to publicly enforced audit, warning, reprimand, corrective order and fine by the regulator.

6. WHAT ACTIONS WILL BE TAKEN

6.1 Compliance will Data Protection Legislation will continue to be monitored by the Information Governance Group. Updates on actions will be provided via the Information Governance Group.

7. LINK TO THE LEADERSHIP DIRECTION

7.1 Supports the objective to become a customer focused organisation under the strategic priority of becoming a more efficient and effective Council.

8. CONSULTATION

8.1 None

9. LEGAL IMPLICATIONS

9.1 HDC must comply with the law concerning FOIA/EIR and Data Protection Act

10. RESOURCE IMPLICATIONS

10.1 There are no direct resource implications arising from this report.

11. OTHER IMPLICATIONS

11.1 None

12. REASONS FOR THE RECOMMENDED DECISIONS

12.1 This paper provides Members an oversight of arrangements in place to ensure Data Protection Compliance.

12.2 This report is for information purposes only, unless otherwise.

13. LIST OF APPENDICES INCLUDED

13.1 None

14. BACKGROUND PAPERS

14.1 None

CONTACT OFFICER

Madelaine Govier
Information Governance Manager & Data Protection Officer (3C ICT)
Infogov@3csharedservices.org