HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Annual report on HDC compliance with the Freedom of Information (FOIA) & Environmental Information Regulations (EIR) Acts
Meeting/Date:	27 April 2022
Executive Portfolio:	Executive Councillor for Corporate Services
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 under the Freedom of Information Act 2000, (FOIA) the Environmental Information Regulations (EIR) the Data Protection Act 2018 and the UK GDPR;
- data protection compliance advice; and
- information and records management advice.

The team is headed up by the Information Governance Manager who is also the Data Protection Officer for the three councils.

This is an annual report on the Council's compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

This report also includes the Councils performance with regard to protecting personal data and covers the period Jan 2021 to Dec 2021.

The number of requests received by the Council in 2021 was 460; a decrease on the previous years total of 534 (a 14% reduction).

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 an update on Information Governance activity and performance during 2021 (January – December); hereby, highlight any issues encountered and actions to be undertaken to improve performance.

2. SCOPE

2.1 It provides:

- An overview of the current arrangements in place to monitor the Information Governance at the Council.

- An update on performance relating to:
  - Freedom of Information (FOI) Act / Environmental Information Regulations (EIR) Requests
  - Data Subject Rights Requests
  - Personal Data Breaches

3. BACKGROUND

3.1 Information is a vital asset and needs to be managed securely by the council. Appropriate policies, guidance, accountability and structures must be in place to manage the council's information legally, securely and effectively in order to minimise risk to the public and staff and to protect its finances and assets.

3.2 Information Governance describes the holistic approach to managing information by implementing processes, roles and metrics to transform information into business assets. This includes access to information, data quality, information management, information security and information sharing, all of which input into data protection compliance.

4. ORGANISATIONAL ARRANGEMENTS

4.1 In addition to the services details in the executive summary on page 1, the Information Governance Service work closely with 3C ICT on information security matters.

4.2 The IG Team consists of six members:

- The Data Protection Officer/Information Governance Manager (who will have been in post for 6 months at the time of this meeting) manages and oversees the service, and provides specialist advice on complex matters around data protection and information management for all three councils.
- The Deputy Data Protection Officer who provides cover and supports the team in the absence of the DPO and is also responsible for the information asset registers for the three councils and supports the information governance officers.
- Three Information Management Officers (one assigned ot each council) who support the Information Governance Officers with complex information requests and also provide advice and guidance to the councils internal departments on matters relating to data sharing, data protection impact assessment and personal data incident investigations.
- Two part time Information Governance Officers who manage incoming information requests and coordinate internal requests for support around personal data incidents/breaches, advice on data sharing and data protection impact assessments/contract reviews.

4.3 As this is a shared service, the Data Protection Officer (DPO) is the statutory DPO for all three authorities.

4.4 Updates on IG arrangements across Huntingdonshire District Council (HDC) are provided to the Information Governance Group (IGG). This Group is designed to facilitate the necessary engagement to ensure the relevant accountability of staff across the various services and to assist in driving any improvements required. It is chaired by the Senior Information Risk Owner (SIRO) and comprises of managers / heads of services across most service areas within the Council.

4.5 The Information Governance Group meets quarterly and last met in February 2022.

5. DATA PROTECTION COMPLIANCE

5.1 As the DPO is new in post a report is in the final stages of completion around progress on data protection compliance against the previous plan and a health check across the information governance service and the three councils, in line with the ICO's compliance monitoring framework. The results of this report are due to be presented at the April/May board.

The initial findings from the review show that, whilst some procedures are in place, and required policies are in place, some of those in place are inconsistently applied/in need of review. Whilst clearly room for improvement exists, the position is not dissimilar to other local authorities, and the level of commitment to progress remains high and owned at the top of the organisation.

5.2 Improvements were required in the following areas:

Area	High Level Finding	Risk	Progress
Information Asset Registers / Flows	Although some Information Asset records were held by Service areas; we do not hold a central repository. These should be reviewed regularly to ensure information is accurate and held centrally.	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.	Significant progress has been made in this action, with the IAR to be completed by July 2022. This will be centrally managed by the IG team to ensure quality of data.
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 transfers.	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)	Once the IAR task is completed a review of transfer arrangements for data will be undertaken, subject to resources.
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	The risk is that staff are not aware of their obligations and therefore put the Council resources at risk.	Policies and procedures will be prioritised in order of importance and a complete set is anticipated to be in place across all three councils by the end of 2022, subject to resources.

Area	High Level Finding	Risk	Progress
	accessible to all staff as they are not published on the Intranet.		
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 enforce the requirement for refresher training for existing staff.	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.	Learning and Development are looking at the reporting functionality to allow greater understanding of take up of refresher training. The new DPO is meeting with HR representatives to review the existing training modules and look at service area engagement. Further actions are likely to result from this which will be reported to IGG in due course.
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.	A log of information sharing arrangements where IG have been approached for input is now in place. Wider communication is required to ensure this is comprehensive and easily accessible. Additional actions will be required to ensure data sharing arrangements are

Area	High Level Finding	Risk	Progress
			communicated accordingly to relevant teams.
Incorporation of Privacy by Design in Projects	Data Privacy Impact Assessment (DPIAs) are 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.	DPIAs may not be completed and therefore privacy risks may either not be identified / identified in a timely manner.	The new DPO is undertaking a review of the DPIA process and ensuring it is linked appropriately to ICT services requests for projects, software and other relevant areas; procurement processes; business transformation processes and all other relevant business areas. This will be in place by Aug 2022.

5.3 The actions to address the above will be factored into the ongoing IG forward plan 2022/23. It is likely that limited progress has been made with the previous plan due to a number of factors:

- Lack of consistency in the role of the DPO/IG manager; there have been 5 postholders in 5 years.
- Considerable volumes of reactive work around complaints from customers. (7 cases across two authorities, including one tribunal case, two ICO cases and several complaints).
- Limited resource required to deal with reactive and proactive work rather than definition between the two.

5.4 Updates to monitor the status and progress of the plan will be provided to the Council's Information Governance Group (IGG) on a quarterly basis.

6. PERFORMANCE UPDATE

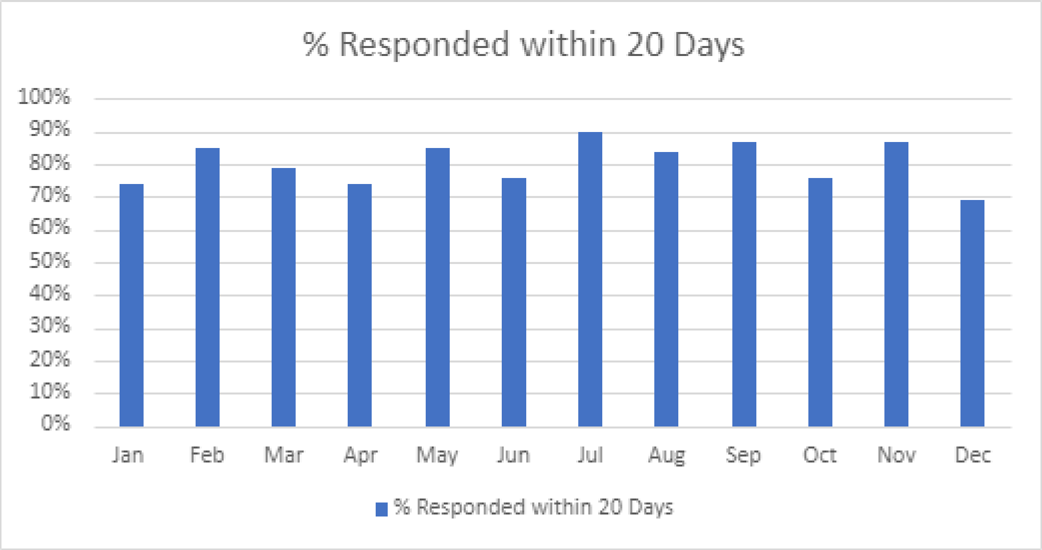
6.1 FREEDOM OF INFORMATION / ENVIRONMENTAL REQUESTS

The public has the right of access to information held by the Council under the Freedom of Information Act. The Freedom of Information Act (FOIA) works alongside the Environmental Information Regulations (EIR).

6.2 Freedom of Information requests relate to requests for information that are not dealt with as part of the day-to-day business processes.

6.3 The 3C ICT Information Governance has implemented a shared request management system for handling information requests. Ownership of the response to these requests is placed on service areas by means of key responders and champions being designated and responsible for ensuring their service responds within the legal timeframe of 20 working days. An Information Governance Officer coordinates all formal requests and allocates specialist support from the Information Governance team where service areas require this.

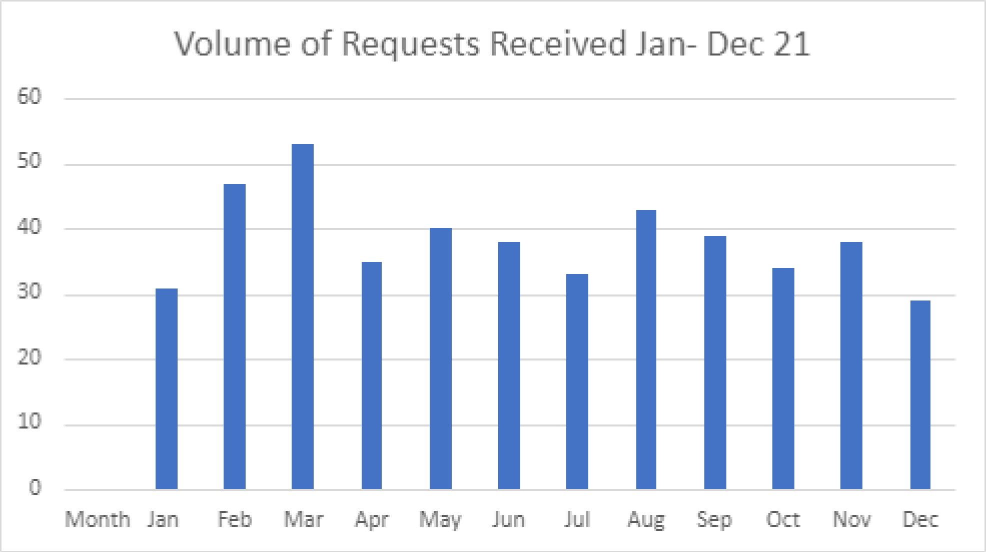
6.4 The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner. We achieved 81% in 2021 which is an improvement on the 77% of the previous year. Breakdown for each month in 2021 is provided below.



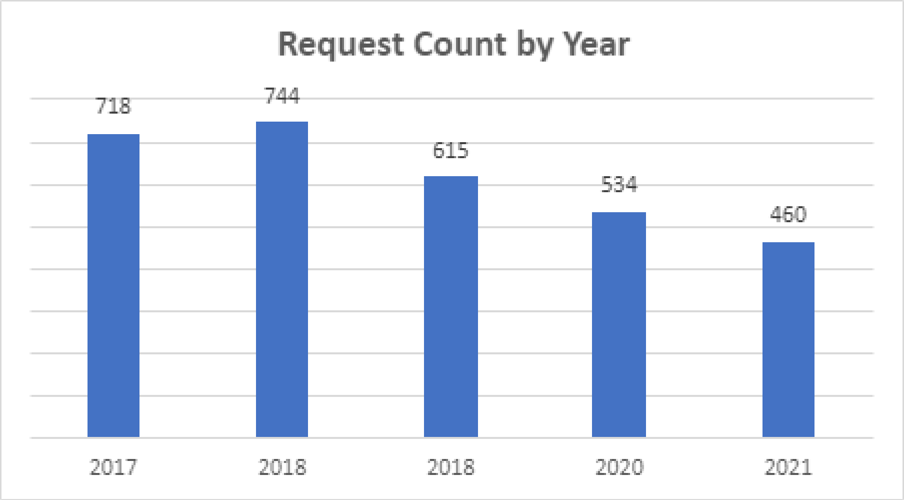
6.5 Reasons for this included service areas not being able to respond to requests for data on time due to priorities being diverted as a result of COVID-19.

6.6 The importance of responding to these on time and correctly is also being reinforced through the Information Governance Group Meetings.

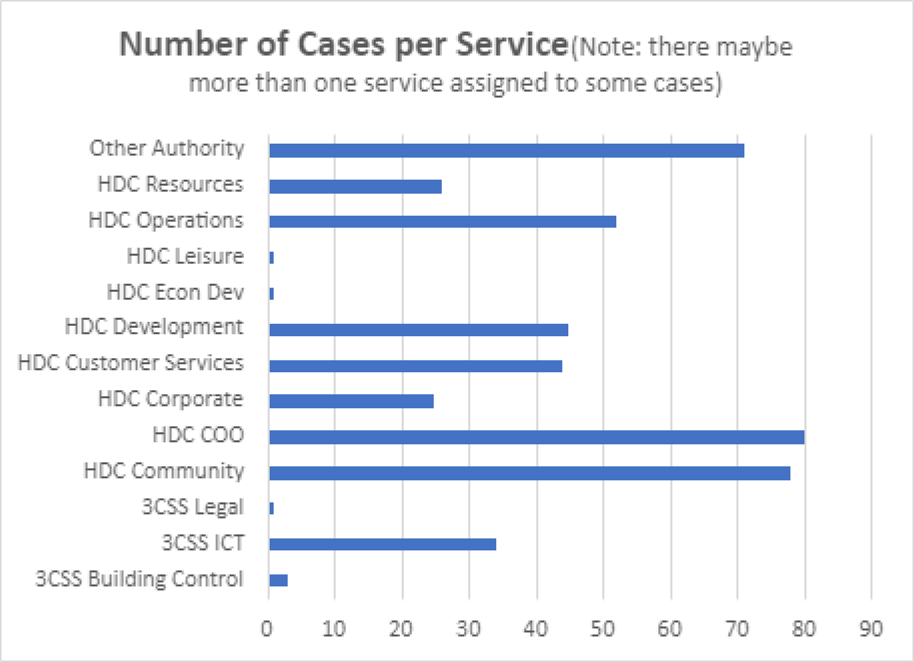
6.7 For 2021 (Jan – Dec) the council received a total of 460 requests under FOI and EIR.



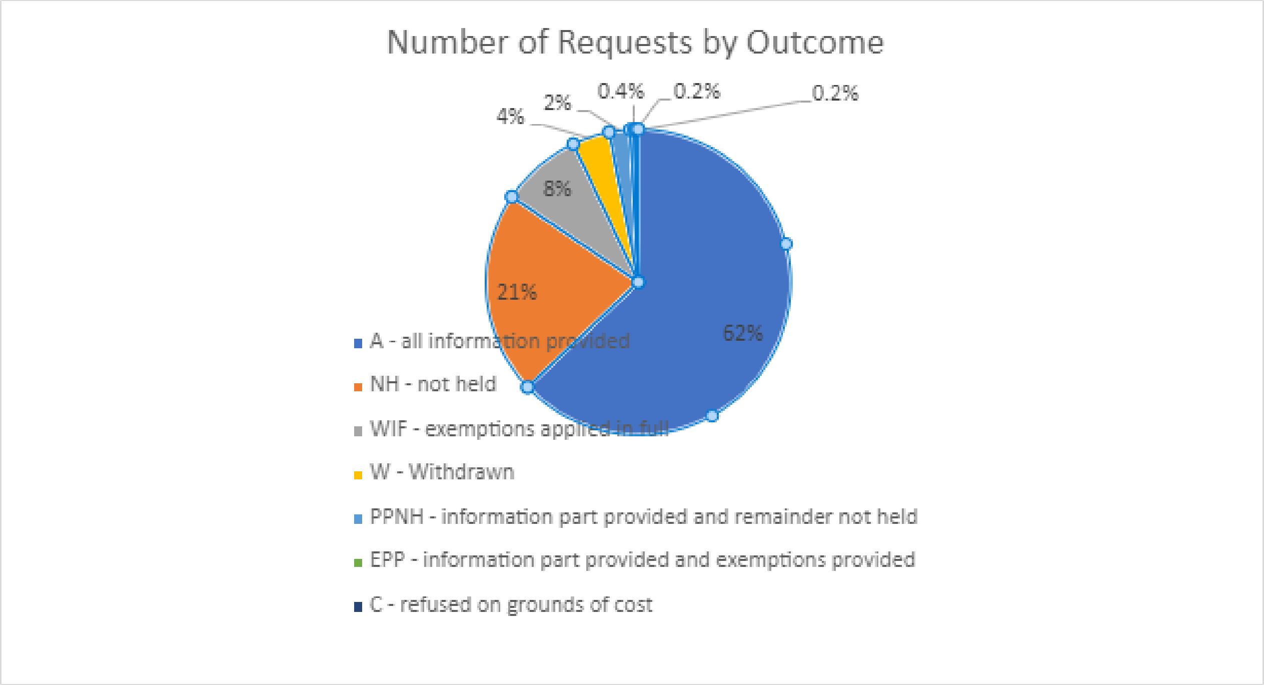
6.8 This represents a 14% decrease in the number of requests received in 2020. The graph below demonstrates the year on year trend in the number of FOI requests received since 2017.



6.8.1 The Chief Operating Officer services and community services have received the most cases. This is also reflected in the volume of late requests (i.e. more requests mean less likely to hit target timescales).



6.11 All the information was provided for the majority of requests. See breakdown of outcomes below.



6.12 The IG team continue efforts to support Services to increase this transparency offering via an Open Data Strategy.

6.13 The IG team continue to provide reports, which are shared with the Information Governance Group on a quarterly basis, to understand trends, and to help departments focus on what should be uploaded onto their publication scheme.

6.14 Requestors have the right to an 'internal review' of their case if they are not satisfied with the outcome or how the request was handled, before taking further action to the Information Commissioner's Office.

	Received
Internal Reviews / Complaints	4
ICO Investigations	6

Whilst there have been investigations by the regulator (ICO) these have resulted in no further action to date.

7. INDIVIDUAL DATA REQUESTS

7.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR). Data protection is primarily concerned with personal data about individuals rather than general information.

7.2 The Information Governance Team coordinate requests relating to individuals rights such as right to request access to the personal data the Council holds, right to erasure, right to rectification as well as third party requests for personal data such as from the Police or to prevent or detect fraud.

7.3 Individual requests made during the year were as follows:

Other Requests	Received	Compliance with time frame
Subject Access Requests (SAR) (including Erasure Requests, etc.)	25	5 (+5 on hold)
SAR Complaints	1	0

7.4 Reasons for delays included:

- lack of awareness by service area officers around the ability to put requests on hold whilst awaiting identification or clarification;
- resources being diverted due to COVID.

The importance of prompt response and the need for training of all staff is also being reiterated through IGG, as well as additional training for Information Champions which will be rolled out in 2022/23 on a quarterly basis.

A review of the current Subject Rights request process is underway to ensure consistency and efficiency in handling these requests.

8. PERSONAL DATA BREACHES

8.1 The guidance on notification of data breaches under the Data Protection Act / GDPR is that where a breach incident is likely to result in high risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours of becoming aware of the issue. If it's likely to result in high risk to rights and freedoms of individuals, the Council has a lawful duty to inform the individuals without undue delay.

8.2 As result, the IG team have established a framework to ensure that each reported incident is assessed for:

- The potential detriment and adverse effect to the data subject. This includes emotional distress and information about the private aspects of a person's life becoming known to others.
- The extent of detriment. Which could depend on the volume of the data and its sensitivity.

The assessment is carried out by the IG team when an incident is logged by a Service Area.

8.3 The IG Team have also developed a register to log incidents / near misses relating to personal data. This allows trends to be identified, with the view to establish if any specific training needs are required or if any actions are needed to enhance the current measures to prevent the likely reoccurrence.

8.4 **Performance Data – Data Breaches**
Although 17 incidents were reported in 2021 (Jan – Dec) only 1 of these met the threshold for reporting to the ICO. A breakdown of these is as follows:

Type of Incident (Category)	Number	Reported to ICO
Personal details inappropriately disclosed (e.g. via email/ shared/published on website)	16	1
Lost or stolen hardware	0	0
Technical Security failing	1	0
Total	17	1

8.5 In all instances, immediate steps were taken by officers to mitigate the incident, once known. Examples included contacting incorrect receiver of emails from the recipients of the email and those affected and removing documents from the Council's website.

8.6 A quarterly update on incidents is provided to the IGG to ensure visibility and ensure any improvements needed are discussed and followed through as appropriate. Where relevant learning from breaches/incidents/near misses is also shared across the three councils to minimise the risk of further occurrence.

9. TRAINING

9.1 To ensure organisational compliance with the law and relevant guidance relating to Information Governance (IG), all council staff and elected members must receive appropriate training.

9.2 A review of e-learning modules, and roll out of annual refresher is due in 2022, lead by the council's new DPO.

9.3 In addition to this, all new starters who manage confidential information are expected to undertake training on handling confidential information.

10. LOOKING FORWARD

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

10.2 The Information Governance team will continue to work with Service areas to address gaps identified as part of the original gap analysis and subsequent health check report (on Data Protection Compliance) and provide updates during the Information Governance Group meetings.

11. KEY IMPACTS/RISKS

11.1 The key impact of non-compliance with FOIA/EIR and the Data Protection Act along with GDPR is public scrutiny from the regulator.

11.2 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.

11.3 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/or fine by the regulator.

12. WHAT ACTIONS WILL BE TAKEN

12.1 Compliance will Data Protection Legislation will continue to be monitored. Actions as identified in Section 5.3 will be undertaken. Updates will be provided via the Information Governance Group.

13. LINK TO THE LEADERSHIP DIRECTION

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

14. CONSULTATION

14.1 None

15. LEGAL IMPLICATIONS

15.1 HDC must comply with the law concerning FOIA/EIR and UK GDPR/Data Protection Act 2018.

16. RESOURCE IMPLICATIONS

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

17. OTHER IMPLICATIONS

17.1 None

18. REASONS FOR THE RECOMMENDED DECISIONS

18.1 This paper updates Members on how requests under FOIA/EIR/DPA have been dealt with by HDC.

18.2 This report is for information purposes only.

19. LIST OF APPENDICES INCLUDED

19.1 None

20. BACKGROUND PAPERS

20.1 None

CONTACT OFFICER

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