Yorkhill Housing Association **AGENDA ITEM 5.3**

Report to: Management Committee – 11 February 2021

Prepared by: Stewart Pattison – Compliance Manager

Subject: Notes to the Freedom of Information/Data Protection Risk Register February 2021

---

1. Purpose of Report

1.1 The purpose of this report is to provide contextual updates to the risks and controls in the Association's General Data Protection Regulation (GDPR) Risk Register; and for inclusion of the risks associated with Freedom of Information. For the purpose of this report Freedom of Information includes Environmental Information. The risk register is appended to this report. The last GDPR update was submitted to the Governance and Finance Sub-Committee on 23 January 2020.

1.2 The risks noted include for those associated with key principles of the General Data Protection Regulation and additional identified risks.

Summary:

Net risks lowered since last assessment	**0**	**Net Risk Scores**	*Number of risks*
Net risks increased since last assessment	**0**	***Risk level low 1-9*** Existing controls sufficient	***9***
No change to net risk score	**10**	***Risk level medium 10-19*** Controls may require review	***1***
New risks added to register	**0**	***Risk level high 20-25*** Controls may be inadequate	***0***
Risks removed from register	**0**		

Notes

		Net Risk Scores
1.	**Lawfulness** The Association has its Compliance Manager as its designated Data Protection Officer (DPO). The DPO ensures the Association is aware of, and complies with, data protection and freedom of information requirements.	**8**
2.	**Unfairness/Discrimination** The Association has an approved Equality and Diversity Policy.	**6**
3.	**Transparency** Privacy Policy and Privacy Statements are in place. The Association's ethos favours information disclosure.	**2**
4.	**Data Fit for Purpose** Staff are aware that information should only be kept for specific purposes. A data cleansing exercise will be undertaken during the implementation process for the new IT system which should include for retention scheduling.	**6**
5.	**Purpose limitation** Retention schedules are in place. The new IT system will include for the right to be forgotten requirement.	**4**
6.	**Security** Passwords are used by staff and housekeeping rules have been distributed to staff. IT security is in place. See IT risk register.	**8**
7.	**Accountability** Data Protection and Freedom of Information/Environmental Information policies approved. Data sharing agreements obtained as required. A records of data incidents is maintained. The Association has a designated Data Protection Officer (DPO) in place.	**2**
8.	**Breaches** The Data Protection Officer maintains a recordable incident register and provides updates to the Governance and Finance Sub-Committee.	**12**
9.	**Subject Access/Freedom of Information and Environmental Information Requests – Staff Resources** The Association's designated DPO monitors staff resources and reports to the Governance and Finance Sub-Committee.	**4**
10.	**Current Information Technology** The Association is currently engaged in an IT procurement exercise.	**6**

Yorkhill Housing Association Limited **FOI/GDPR Risk Register** **February 2021**

No.	Risk	Gross Lhd (1-5)	Gross Imp (1-5)	Gross Risk Total	Managed by key systems/processes	Lead	Net Lhd	Net Imp	Net Risk Total	Action Required
1	Lawfulness.	3	4	12	Keep abreast of regulation and legal requirement and any changes/breaches elsewhere.	DPO	2	4	8	Keep up to date with bulletins. SFHA, GWSF, ICO, SIC, Government Guidance.
2	Unfairness/ Discrimination.	3	4	12	Equalities training to be undertaken when restrictions eased. Equality and Diversity Policy September 2019.	DPO	2	3	6	Ensure staff are fully trained. Policy acknowledgements. Review systems.
3	Transparency.	2	3	6	Privacy policy; Privacy statements; Working practices. Freedom of Information/Environmental Information policies.	DPO	1	2	2	Policy available, statements distributed. Newsletters, Internet.

4	Data fit for purpose.	3	3	9	Ensure data is collected for specific purposes, limited to what's needed and accurate. New IT system functionality.	All staff	2	3	6	Staff training, information audits, reviews.
5	Purpose limitation.	3	3	9	Retention schedules. New system functionality.	Mgrs.	2	2	4	Review retention schedules.
6	Security.	3	4	12	Passwords; encryption; housekeeping rules; systems. Cyber security application being progressed.	Mgrs.	2	4	8	Continual review; change passwords as scheduled; observation and supervision by managers.
7	Accountability.	2	3	6	Implementing Data Protection/Freedom of information and Environmental Information policies. Data sharing agreements.	DPO	2	1	2	Monitoring and review.

					Implementing security measures. Recording data incidents or breaches. Risk register.					
8	Breaches.	4	4	16	Policies and procedures. Protocols. Recordable Incidents log. Log includes action taken.	DPO	4	3	12	Incident register developed and maintained. Housekeeping rules. Data sharing agreements. Addendums for contractors and other service providers. Data Protection Policy. Requires ongoing review.
9	Subject Access Requests. Freedom of Information Requests Environmental Information Requests. Staff resources. Statutory timescales.	4	3	12	Data minimisation ethos. Time management. Set timelines provided.	DPO Mgrs. DPO	2	2	4	Monitor requests and resources expended. Report to Governance and Finance Sub-Committee. SIC return.

										Reports to Governance and Finance Sub-Committee.
10	Current Information Technology capability. Data migration to new system. Right to be forgotten (Current legacy system).	4	3	12	IT System upgrade. System functionality.	FMgr DPO	2	3	6	Implementation of IT upgrade. Committee approval required. Procurement exercise progressing.

Summary of FOI/GDPR net risk score

I	**5**					
M	**4**		**2**			
P	**3**		**3**		**1**	
A	**2**	**1**	**2**			
C	**1**		1			
T		**1**	**2**	**3**	**4**	**5**
PROBABILITY						