GDPR PROJECT PLAN SUMMARY – 3 JANUARY 2018

ACTIONS	OWNERS (to be agreed with officer Steering Group)	COMPLETION DATE
1. First meeting of steering group		COMPLETED Nov '17
2. Phil's launch note		COMPLETED Dec '17
3. DPA Training & Policies online		COMPLETED Dec '17
4. All staff complete training/read policies online		BY MID JAN '18 LATEST
5. Obtain ECC GDPR presentation		BY MID JAN '18
6. Members invited to complete online DPA training		BY END JAN '18
7. Prepare/send out questionnaire, guidance notes and data mapping exercise to all departments to complete and return to DPO (see further below for follow up action)		EARLY FEB '18
8. Roll out ECC GDPR presentation to senior staff/all managers		DURING FEB ' 18
9. Prepare updated progress report for PP&R Committee		BY 1/3/18 LATEST
10. Review IT compliance with GDPR requirements (SEE IT SPECIFIC ACTIONS/QUESTIONS BELOW)*		DURING MARCH/APRIL 2018
11. Check all responses to 7 above received then meet with steering group to allocate work streams/agree completion dates as necessary around requisite changes to contracts, data processor agreements, Privacy Notices, Privacy Impact Assessments, appointment of DPO, Data Breach Policy and any other areas identified from responses		BY MID MARCH '18 LATEST
12. Ensure all workstreams identified under 11 above		BY 25 MAY '18 LATEST

completed		
13. Amend annual registration payments as directed by ICO in due course		TBC
14. Appoint the Data Protection Officer		BY 25 MAY ’18 LATEST
15. Ensure Data Breach Policy in place		BY 25 MAY ’18 LATEST
16. Update DPA policies to reflect GDPR/new procedures being followed		BY 25 MAY ’18 LATEST
17. Conduct GDPR compliance audit/make necessary changes to ensure reasonable compliance achieved		BY END MAY ’18

* “IT SPECIFIC ACTIONS/QUESTIONS”

- Are our systems safe, secure and fit for purpose? For example, secure against cyber attack?
- Under GDPR’s “right to be forgotten” do all our systems enable erasure of personal data on an individual basis?
- Do we/can we pseudonymise or anonymise personal data?
- Consider email deletion policy (auto-deletion) after say 1 year of all emails not saved outside of Outlook.
- Can we always produce a person’s personal data electronically and in a ‘commonly used format’?
- Encryption arrangements satisfactory?
- Cyber Security arrangements satisfactory?
- Other threats to IT security identified and actions to be taken?