Training & Awareness Procedure

Title	Training & Awareness Procedure
Status	Approved
Version	V1.0
Date Approved	November 2019
Review Date	November 2020

Contents

1. Quick guide to training requirements

Task	Detail and resources
Induction Training	All staff must complete induction training. Such training as a minimum should include: • General data protection requirements • Physical and technical security practices • Policies and procedures • Individuals rights regarding their personal information • Who to go to for advice • Business continuity arrangements Induction training must be logged on your reporting tool and relevant records retained as evidence Appendix 1 & Appendix 2 can be used to inform training and awareness.
Annual eLearning	All staff must complete the GDPR eLearning module annually and your reporting tool updated to provide evidence.
Specific Training	Make sure that any additional training is relevant to the roles of individuals
Awareness communications	Outcomes from security incidents should be analysed and where appropriate learning from incidents shared with staff via email or staff briefings. Changes to policies, processes or legislation should also be communicated to staff in a timely manner and logged on your reporting tool.
Feedback	Feedback should be sought after training events and used to improve the effectiveness of the training provided.

2. Introduction

Training and awareness around employee responsibilities when handling personal data is a key element of GDPR. The Regulations consider the

effectiveness of training to be a key consideration in whether an Organisation can claim that its measures to keep personal data secure are ‘appropriate’.

This procedure outlines an approach to ensuring employees are effectively trained and aware of how to manage personal data

Please see Appendix 1 for a briefing note that could be provided to all employees as a basic guide to the key aspects of GDPR

Please see Appendix 2 for a guidance document that can be provided to parents/ guardians to help promote transparency and awareness on the GDPR rights

3. Policy References

3.1. This procedure is a requirement of the following policies:

- Data Protection Policy

4. Procedures

4.1. Training relevant to Roles

4.1.1. Training needs should be identified and linked to roles across a School. For example, a School may identify the following roles: Teaching staff, Office staff, Leadership roles and Volunteers. In addition there may be roles held by individuals with increased responsibilities e.g. a Data Protection Officer, Business Manager, Safeguarding Officer, Special Needs Co-ordinator, Senior Risk Owner, a Governor with a specific Data Protection remit etc.

4.1.2. The school will need to decide whether:

a) The same training can be delivered to all staff (and perhaps be supplemented by additional training for key roles), or
b) Training needs to be tailored for each role (so that each role has training content specific to their activities)

4.1.3. The School needs to document the approach it has chosen in its Security Measures (Document H2 of this Framework)

4.2. Induction

4.2.1. Arguably personal data is most at risk when it is being handled by people newly recruited by the School who are not yet familiar with the correct procedures. It is therefore important to be able to introduce a 'new starter' to the School's Information Governance policies, procedures and guidance as soon as possible before they are given access to personal data.

4.2.2. An effective way of ensuring that induction messages are delivered consistently and fully is to work with a standard induction checklist form. This should confirm that:

a) Policies, procedures and guidance are relevant and that they have been shown where they can find them.
b) Key information systems have been demonstrated and they have seen how these should be correctly used.
c) If relevant, they have been shown the Asset Register and Data Flow Mapping document so that they can see how the School expects certain types of data to be handled and disclosed to external bodies and individuals

4.2.3. Once induction has been successfully delivered, the member of staff delivering this should sign to confirm delivery, the new starter should sign to confirm receipt and the checklist (or a copy) should be filed on the new starter's employee record.

4.3. Refresher Training

4.3.1. It is important to make sure that employees are reminded of their Data Protection responsibilities within a reasonable frequency. The law doesn't specify how frequently training should occur but it would make the wider tasks of reviewing your Data Protection practices more manageable by setting an expectation that employees do refresher training annually.

4.3.2. It is recommended that anyone who deals with personal data in their day-to-day roles should see the requirement to undertake refresher training as a mandatory requirement. Managing this could form a part of annual appraisals of employee performance in order emphasise the status in which the School regards the requirement.

4.3.3. The law does not specify how training should be delivered; only that it is effective. Training therefore doesn't have to be delivered face-to-face, it can be done by other means such as through eLearning. There are many providers of online modules covering GDPR content. If any training is externally sourced, it should be reviewed and confirmed as appropriate.

4.4. Recording and Reporting

4.4.1. GDPR introduces a requirement to evidence compliance activities and training records are expected to form a part of this. For example, in the event of a security breach caused by an employee, being able to evidence that the individual had received the right instruction through training on how to avoid the breach could provide the ICO with important assurance that may significantly reduce the likelihood of regulatory action against the Data Controller. Evidence that such training was delivered on induction and at regular intervals during their employment would form a strong part of an argument that the School had taken reasonable efforts to prevent the breach form occurring.

4.4.2. Records of training activities can either be kept on individual employee files or be kept in a central training record which covers all employees.

4.4.3. If training is to be mandatory, as is the strong recommendation, then information about how many employees have successfully completed training should be reported. One of the Data Protection Officer's roles is to be assured that appropriate training is taking place. In order for the DPO to effectively give their opinion to the School on how well it is complying with the law, it is important that the number of employees being successfully trained forms a part of the performance data that they can review and comment upon

4.5. Reviewing

4.5.1. Feedback: In order to ensure the content of the training is delivering the right messages, it is important to regularly consider employee feedback. Every instance of training should be accompanied or promptly followed by giving the trainees the opportunity to rate, constructively criticise and suggest improvements to training.

4.5.2. Security Incidents: A review of training effectiveness should also include a review of trends in security incidents. Several incidents relating

to the same type of failings would indicate that either employees are not effectively taking-in and remembering the training messages that would prevent the breaches, or that existing training was not covering these incidents.

4.6. Awareness

4.6.1. Employee reminders about how to effectively manage personal data should not be limited to formal training activities. Reminder memos, briefings on new guidance, messages around specific risks or security incidents are all examples of ad hoc awareness-raising. These too are examples of good practice where the School is making the effort to ensure that Data Protection issues are taken seriously. Examples of these communications are also important to keep as part of the School's evidence of its compliance activities.

5. Advice and Support

5.1. If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact the school office.

6. Breach Statement

6.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 1: GDPR Guidance - Employee Briefing

This is a guidance document to employees summarising the key points of GDPR. It is designed as easy-to-consume one page points, but allowing the reader to click links to expanded detail if they wish.

Evidence should be kept of who received the document and when in order to contribute to a complete record of Training and Awareness delivered to staff.

11A. GDPR Guidance - Employee Briefing v.

Appendix 2: GDPR Rights - Advice to Parents/ Guardians

This document is aimed at promoting awareness among parents and guardians. The document gives them a brief introduction to their rights, when they apply and how they can expect the School to manage their requests. This could be sent direct to parents/ guardians in paper or digital format, but could be published on the School website with parents/ guardians provided with a link to it from a regular newsletter/ flyer.

GDPR Rights - Advice to Parents-Guardians