

West Exmoor Federation



Privacy Impact Assessment Procedure

Version 1.0

Document Date: December 2018
West Exmoor Federation
(Lynton CE Primary)
(Parracombe CE Primary)
(Kentisbury Primary)

If you require help in the interpretation of this procedure, contact the Information Governance Team at keepdevonsdatasafe@devon.gov.uk

1.0 Introduction

1.1 This procedure supports the School's Data Protection Policy and applies to staff, agents, Governors, contractors and partners of the School. The intention of this procedure is to ensure that Devon County School is able to identify and manage information risks in a manner that ensures compliance with the requirements of [Article 25](#) (privacy by design) of the General Data Protection Regulation (GDPR).

2.0 Scope

2.1 This procedure applies to those undertaking a [privacy impact assessment](#). This may include members of staff members, contractors or those under the direct supervision of the Data Protection Officer.

3.0 Procedure review

3.1 This procedure will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer at West Exmoor Federation

4.0 Roles and responsibilities

4.1 Responsibility for GDPR compliance rests with the School's Senior Information Risk Owner (SIRO). The Data Protection Policy and its supporting guides and standards are managed, maintained and communicated to staff by the Data Protection Officer.

4.2 The School's Information Asset Owners and Information Asset Administrators are responsible for ensuring that appropriate structures and procedures are in place to enable the School to manage requests from data subjects to exercise their rights under the GDPR. They are also responsible for ensuring that staff are made aware of, and comply with the Data Protection Policy, its associated standards and the Privacy Impact Assessment Procedure. All staff are personally responsible for complying with this policy and supporting standards.

4.3 Requests to exercise should be directed to the Data Protection Officer who is responsible for oversight of these requests.

5.0 When to conduct a privacy impact assessment

5.1 A [privacy impact assessment](#) is designed to identify risks that might adversely affect someone's privacy, or which may affect the ability of the School to comply with the requirements of the GDPR. It also seeks to propose ways to eliminate these risks or reduce them to an acceptable level. Circumstances which will require a [privacy impact assessment](#) are outlined below.

- In response to [a security incident](#) where a data protection breach has occurred
- When there is a proposal to use [personal data](#) in a way that is not compatible with the original purpose for which it was obtained
- When designing new systems or ways of working, involving the processing of [personal data](#)

- Prior to procuring goods and or services where the processing of [personal data](#) is intended to take place
- In circumstances as directed by the Data Protection Officer

5.2 Privacy impact assessments may be undertaken by any School employee under the supervision of the Data Protection Officer.

6.0 Risk monitoring

6.1 All completed privacy impact assessments will be reviewed by the Data Protection Officer who will ensure that risks identified are recorded on the School's Information Risk Register and are monitored in accordance with the School's Information Assurance Policy.

7.0 Risk mitigation and reporting

7.1 Once suitable proposals to mitigate any risks identified in a [privacy impact assessment](#) have been ratified by the Data Protection Officer, a completed privacy impact assessment report with recommendations to reduce those risks, will be communicated to the following personnel, depending on the level of risk identified from each assessment.

Risk classification	Description of risk	Report to
High Risk	The proposed activity is more likely than not, to adversely affect the rights and freedoms of those personal data is to be processed.	DPO, Vikki Brown Headteacher, Jayne Peacock ICO
Medium Risk	The proposed activity may adversely affect the rights and freedoms of those whose personal data is to be processed.	DPO, Vikki Brown Headteacher, Jayne Peacock ICO
Low Risk	The proposed activity is unlikely to result in an adverse affect on the rights and freedoms of those whose personal data is to be processed.	DPO, Vikki Brown Headteacher, Jayne Peacock
No Risk	The proposed activity will not adversely affect the rights and freedoms of a data subject.	DPO, Vikki Brown

7.2 Decisions on whether to accept mitigations proposed in a privacy impact assessment are to be made by those identified in the table above. Any residual risks which remain classified as High Risk following the application of any risk mitigation activities, are to be reported to the Head Teacher, the Data Protection Officer and the [Information Commissioner's Office](#) in accordance with the requirements of [Article 36](#) of the GDPR.

8.0 Privacy impact assessment record keeping

13.1 The officer responsible undertaking a [privacy impact assessment](#) will ensure that robust records are kept of their handling of each assessment. Where possible, any investigation will be informed by discussions with key personnel. Records will be retained for the duration of the security incident investigation and in accordance with the School's Corporate Retention Policy.