

REPORTING OF PERSONAL DATA BREACHES POLICY and PROCEDURES

Contents

Document Control.....	1
Policy and Procedure Statement	2
Purpose	2
Scope.....	2
Definitions.....	3
Risks.....	3
Procedures for reporting data breaches	4
Policy and Procedure compliance.....	5
Policy & Procedure Governance	6
Appendix I – Process Flow: Reporting a personal data Breach.....	7

Document Control

Version	Date	Author	Comments
1	April 2018	ICT Audit and Compliance Manager	GDPR Compliance
2	August 2018	ICT Audit and Compliance Manager	
3	April 2021	ICT Audit and Compliance Manager	Update Review
4	August 2023	Data Protection Officer	Legislation & procedures review

Policy and Procedure Statement

The Partner 'Councils': Cotswold District Council, Forest of Dean District Council and West Oxfordshire District Council will seek to avoid personal data breaches. Each Council recognises a personal data breach if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned.

Where personal data breaches do occur the Councils will, without undue delay, seek to contain the harm to individuals, investigate the breach, report the breach to the Information Commissioner's Office (ICO) within 72 hours and look to learn the lessons from any actual or suspected breaches.

Purpose

This Policy explains how the partner Councils and Publica complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the Information Commissioner's Office (ICO) and the affected individuals in accordance with the Data Protection Legislation (UK . The partner Councils and Publica have a Data Breach Notification Procedure and Data Breach Register that set out how we deal with and record Personal Data breaches.

Scope

This document applies when a personal data breach is suspected. The policy and procedure it sets out is to be followed by:

- Councillors.
- Committees.
- Services.
- Partners.
- Employees of the Council.
- Contractual third parties and agents of the Council who use ICT facilities, or who require remote access to the Council's Information Systems or information.

This Policy should be applied with appropriate reference to the Council’s ‘General Data Protection Regulation Policy’ and the ‘Information Security Policy’ including, but not restricted to, the following contents within the Information Security Policy:

- Data Protection Polices
- ICT Acceptable Use Policy (Signed)
- Access Control.
- Card Payments Standards.
- Email Usage.
- Incident Management. .
- Information Security Standards.
- Equipment Usage.
- Internet Usage.
- Removable Media.
- Reporting of Breaches Procedures.
- Software Security
- Information Protection Handling and Guidance
- Agile Working Policy.
- Members Guide to Use of Information Technology
- Cyber Incident Response Guidance

Definitions

“**Personal data**” means any information relating to an identified or identifiable individual (‘data subject’); an identifiable individual is someone who can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

A “**personal data breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach includes, but is not restricted to, the following:

- The accidental alteration or deletion of personal data;
- The transfer of personal data to those who are not entitled to receive it;
- Unauthorised access to personal data;
- Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could reasonably have contemplated; and
- Theft of storage devices

Risks

Each Council recognises that there are risks associated with the collection, use, transmission and storage of personal data in order to conduct official Council business. By following this

policy and procedure, suspected personal data breaches should be identified quickly and the impact of personal data breaches should be reduced by ensuring suspected personal data breaches are followed up correctly, and helping identify areas for improvement.

Procedures for reporting data breaches

Appendix I provides a high level process flow diagram illustrating the process to be followed when reporting suspected or actual personal data breaches.

Personal data breaches need to be reported to the partner Council's & Publica Data Protection Officer, for each of the Councils email on:

- Cotswold District Council: data.protection@cotswold.gov.uk
- Forest of Dean District Council: data.protection@fdean.gov.uk
- West Oxfordshire District Council: data.protection@westoxon.gov.uk
- Publica (Support) Ltd - Data.Protection@publicagroup.uk

or call on **01993 861194** at the earliest possible stage as the Councils has a duty to report any personal data breach to the Information Commissioner's Office ("the ICO") within **72 hours** unless the Information Commissioners Office (ICO) has issued guidance to the contrary.

The information provided to the Data Protection Officer should include as much detail as possible of the personal data breach, those affected and the consequences.

When reporting the breach to the ICO the Data Protection Officer will include the following information:

- The nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

In the event that it is not possible to report the personal data breach to the ICO within **72**

hours, the notification will also give the reasons for the failure to do so.

Incident Monitoring and Closure

Each partner Council and Publica will evaluate and review the cause of the breach and effectiveness of the response to it. This will help reveal any systemic or ongoing problems and prevent any future breaches from occurring. Whenever breaches happen, each Council and Publica understands the need to learn any lessons and tighten up security. In most cases, the data breach which involve human error. As a remedial action, the staff member involved will be required to undergo refresher data protection training. Further training needs may be identified and rolled out across the relevant partner Council and Publica.

All breaches will be recorded regardless of whether it needs to be notified to external parties, and the outcomes and decisions made in respect of them is reviewed and recorded with the Chief Technical Officer and the Data Protection Officer and Compliance Officers.

Training & Development

Each partner Council and Publica are committed to ensuring the staff adopt the highest standards in relation to the processing and handling of Personal Data.

All existing staff will be trained annually. New staff and councillors will be trained as part of their induction within 3 months of their joining the Council / Publica and being able to access Personal Data.

Policy and Procedure compliance

If any officer is found to have breached this policy and procedure, they may be subject to the each Council's disciplinary procedure. If any councillor is likewise found to have breached the policy and procedure, a complaint will be made to the Standards Committee. In either case if a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Protection Officer or SIRO.

Policy & Procedure Governance

The following table identifies who within each Council is Accountable, Responsible, Informed or Consulted with regards to this policy and procedure. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Data Protection Officer
Accountable	SIRO / Head of Paid Services / Chief Executives
Consulted	SIRO / Head of Paid Services , Senior Management Team / Chief Technical Officer
Informed	All Councillors, Committees, Employees, Contractors and Agents.

Appendix I – Process Flow: Reporting a personal data Breach

