Data Protection Corporate Policy

Why this Policy matters

This Policy provides a framework for ensuring that we meets our obligations under the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA 18') and the Privacy and Electronic Communications Regulations ('PECR'). It applies to all the processing of personal data carried out by the BBC including processing carried out by joint controllers, contractors, and processors.

We comply with data protection legislation guided by six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines.

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our employees have access to a number of Policies, operational procedures/standards and guidance to give them appropriate direction on the application of the data protection legislation, and this Policy should be used in conjunction with the following policies, procedures/standards and guidelines:

1. Data Protection Handbook
2. Data Protection – How we use your data
3. People Privacy Notice
4. Personal Data Minimisation and Retention Procedure
5. Data Protection Risk Management Guidance
6. Appropriate Policy Document – Our Processing of Special Categories of Personal Data and Criminal Offence Data
7. Information Security Policies
8. Records Management Corporate Policy
9. Records Management Guidelines
10. Corporate Retention Schedule
11. Responsible AI Corporate Policy

The BBC is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about audiences, employees or those who work or interact with us.

Who this Policy applies to

This Policy applies to you if you work for, or represent, the BBC or one of its subsidiaries. This includes, but is not limited to:

- employees, full-time or part-time
- those on a fixed term or temporary contract
- freelancers, contractors or consultants
- volunteers or interns

Overview

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person. Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive (“special category data”) and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences).

We have processes to make privacy by design an integral part of any product, service or process.

The essential things you must do or not do

These high-level essential mandatory requirements are the most important for you to understand and follow to meet the Policy objectives.

In addition to these, there are detailed requirements and best practices outlined in supporting procedures and guidance, linked below. Read this information when you need to understand the detail.

If you have any concerns or conflicting priorities that prevent you following essential requirements, please discuss them with one of the people listed in the section under ‘Where to go for help and exceptions’. Without an approved exception, breaches may put the BBC at risk and may result in disciplinary action, up to and including dismissal, or termination of our relationship with you.

Processing Personal Data

1. You must ensure the secure and compliant processing of any BBC personal data you collect, process and retain.

Data Protection Risk Assessment

2. You must consult the Data Protection Office Team on processing activities that are likely to result in a high risk to individuals.

The team will advise if a **Data Protection Impact Assessment**, **Transfer Impact/Risk Assessment** and/or an **AI Risk Assessment** needs to be carried out. The team will also advise if a **Privacy Notice** is required

Assessing data protection risk at the earliest point in the project life-cycle will ensure risks are identified and adequate controls can be implemented to reduce risk.

Where personal data is transferred outside of the UK, we do a Transfer Risk Assessment to put appropriate safeguards in place to protect the personal data.

Data Security Incident/Breach Management

3. You must notify the Data Breach Investigations Team or the Data Protection Officer immediately if you become aware of an actual or potential personal data breach.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Personal data incidents can have a significant impact on individuals (whether audience, employees or contributors) as well as the reputation of the BBC. All relevant data protection legislation holds the BBC responsible for the careful monitoring, containing and reporting of incidents. This duty affects everyone.

Data Protection Training

4. You must undertake your mandatory Data Protection and Cyber Security training as part of your induction and then retake every two years.

In addition, some roles require employees to attend a more detailed data protection training module(s) as part of their role, such as Enhanced and Advanced Data Protection training.

Information Rights

5. If you receive a subject access request (SAR) or any other information rights request, you must notify the Information Rights Team or the Data Protection Officer.

We have a dedicated team and clear processes to handle SARs and other information rights requests.

Information Security

6. When working with third parties who process personal data on behalf of the BBC, you must contact Information Security to ensure we have the right level of security needed to protect the data.

Information security is a key principle of the UK GDPR and we must secure personal data by appropriate technical and organisational measures.

Ultimately we are responsible for checking that third parties have the level of security needed to appropriately protect the data in line with our requirements. These security concerns relate not only to unauthorised access, but to accidental loss or damage. We will be held accountable for breaches, so we need to make sure these measures are in place. Most third parties will need to complete the InfoSec Holding and Hosting Form.

Contracts

7. If you have a contract for a service that processes personal data on behalf of the BBC, you must contact the Data Protection Legal Team who oversee that our contracts are compliant with the UK GDPR.