DATA PROTECTION POLICY

INTRODUCTION

This policy sets out how the British Copyright Council (BCC) protects Personal Data relating to member representatives, applicants and delegates for WIPO-IPO-BCC courses, consultants working for the organisation and other service providers, stakeholders and members of the public contacting the BCC, and website users.

The BCC is committed to handling data responsibly, transparently, and in compliance with applicable data protection laws. The BCC is registered with the Information Commission as a data controller.

Throughout this Policy, "Personal Data" means data relating to a living individual who can be identified from that data.

This Policy should be read in tandem with the BCC Privacy Notice which is published on the BCC website and which sets out:

- When and why the BCC collects personal data
- The lawful basis for the BCC processing personal data
- How the BCC shares and transfers personal data

SCOPE

This policy:

- Applies to all Personal Data processed by the organisation;
- Covers members, consultants, and any other individuals whose Personal Data is collected; and
- Applies to all systems, paper records, and digital platforms used by the organisation.

The majority of BCC interactions with individuals are on a business-to-business basis, but some interactions are with individuals working in a consultancy capacity for the BCC, a BCC member or another organisation, and with members of the public contacting the BCC in a personal capacity.

ROLES & RESPONSIBILITIES

The roles and responsibilities are as follows:

- Data Controller: The BCC's Executive Administrator determines the purposes and means of processing Personal Data.
- Data Protection Lead: The BCC's Executive Administrator oversees compliance and acts as the contact point for queries.
- Consultants and other service providers: Must follow this policy and refer to the Privacy Notice when handling Personal Data on behalf of the organisation.
- Member representatives: Are expected to respect the Personal Data of other member representatives, applicants and delegates for WIPO-IPO-BCC courses, consultants and other service providers and other stakeholders.

- Applicants and delegates for WIPO-IPO-BCC courses: Are expected to respect the Personal Data of other applicants and delegates.

PRINCIPLES OF DATA PROTECTION

The BCC adheres to the following principles:

- Lawfulness, fairness, transparency – Personal Data is processed legally and openly.
- Purpose limitation – Personal Data is collected for specific, legitimate purposes only.
- Data minimisation – only necessary Personal Data is collected.
- Accuracy – Personal Data is kept up to date.
- Storage limitation – Personal Data is retained only as long as necessary.
- Integrity and confidentiality – Personal Data is kept secure.
- Accountability – the organisation takes responsibility for compliance.

DATA SECURITY

Personal Data is stored on secure, password-protected systems and associated software is kept regularly updated.

Access is restricted to authorised individuals.

DATA BREACH MANAGEMENT

A data breach occurs where there is accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to Personal Data which is being held, stored, transmitted or processed in any way.

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

- Loss, destruction or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record);
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- Unauthorised use of or modification of data or information systems;
- Unauthorised disclosure of sensitive or confidential data; and
- Human errors, such as sending an email to the wrong person.

All actual or suspected data breaches must be reported immediately to the Data Protection Lead together with as much information as possible.

In the event that an email is sent to the wrong person, advice must be sought from the Data Protection Lead before any further action is taken.

Breaches will be investigated and, where required, reported to the Information Commission's Office (ICO) within 72 hours of discovery of the breach.

Affected individuals will be notified if there is a high risk to their rights and freedoms.

If you receive notification of a security incident or Personal Data breach from a third party, the same process as that outlined above must be followed.

DATA DESTRUCTION

The BCC will not keep Personal Data for any longer than is necessary, bearing in mind the purposes for which we collect and use it (as described in the Privacy Notice).

The disposal of Personal Data which are no longer needed will take place as follows:

- Hard copies - shredding
- Electronic – destruction to render such data non-recoverable

REVIEW

This policy will be reviewed annually or sooner if required by changes in law or organisational practice.

DATE: 15 April 2026 (revised to amend name of ICO – 21.10.26)
DATE OF NEXT REVIEW: April 2027