DBS Privacy policy

This privacy policy explains your rights as a customer of the DBS under the Data Protection Act 1998. It explains why we require your personal data, and what you can expect from us in terms of our data protection responsibilities.

About this policy

This policy explains your rights as a customer of the DBS. These rights are set out by the Data Protection Act 1998 (the Act). The policy explains why we require your personal data. It will cover what we do with your data and what you can expect from us in return. It will also explain how to obtain a copy of any personal data we may hold about you.

The policy will not replace the Data Protection Act. It will show how the DBS will comply with the Act when processing your personal data.

The DBS has two functions:

- Disclosure which searches police records and, in relevant cases, information held by the DBS Barring function and issues a DBS certificate to the applicant;

- Barring to help safeguard vulnerable groups including children from those people who work or volunteer with them who pose a risk of harm. The DBS may use any information on a certificate or otherwise held by the DBS to inform any of it's barring decisions made under its powers within the Safeguarding Vulnerable Groups Act 2006.

This policy is aimed at persons using or that have been referred to the Disclosure and Barring Service and sets out their rights.

Your rights and how we protect them

The DBS is committed to compliance with the Act. We hold a legal duty to do so. We will take every precaution to protect your data. The following principles will apply when we process your personal data:

- only data that we actually need is collected and processed
- your data is only seen by those who need it to do their jobs
- your data is retained only for as long as it is required
- your data is accurate and is only used as part of the DBS process
- decisions affecting you are made on the basis of reliable and up to date data
- your data is protected from unauthorised or accidental disclosure
- you will be provided with a copy of data we hold on you, on request
- there will be procedures in place for dealing promptly with any disputes / complaints

- your data with regard to the Disclosure Service is only processed with your knowledge and consent

All will apply whether we hold your data on paper or in electronic form.

What personal data we hold

We will only hold your data if you have:

- applied for a Disclosure check;
- applied to be a Counter signatory for a Disclosure check;
- been referred to the Barring Service

The DBS has access to the Police National Computer (PNC). For the Disclosure function this is basic identifying details such as name and date of birth of persons included on the PNC. For the Barring function access is granted to personal details and conviction information.

The DBS does not capture or store data about visitors to its website. However, you may choose to give us data such as your name, address, or e-mail for enquiries. If this is the case, the data received will be kept for 6 months. The data is kept for this period to allow for any follow up enquiries and/or information.

Responsibility for your personal data

The DBS is the 'data controller' of all data held within the DBS. This means that we hold full responsibility for the safety of the data contained on a DBS Disclosure application form and data held on all referrals to the Barring function.. The DBS is also a ‘data processor’ of the data held by the specified ‘data sources’.

Any organisation that works on behalf of the DBS is referred to as our ‘data processor’. We can assure that our ‘data processors’ comply with the Act. This is to the same high standard as the DBS.

Your information maybe used for testing purposes to ensure that the system functions as per specified requirements and only where dummy data is not practical or the use of data obfuscation or masking could result in referential integrity issues.

Organisations that are involved in the DBS service

Your data will only be seen by those whose jobs require them to do so. In practice, this means DBS staff conducting the various checks that are necessary for the issue of disclosure certificates and decision making. Data may also be passed to organisations and ‘data sources’ involved with the DBS. These are:

- Tata Consultancy Services– a partner in the DBS service.
- Police forces in England, Wales and Northern Ireland, the Isle of Man and the Channel Islands – searches will be made on the PNC and data may be passed to local police forces in the area where you live, or have previously lived. The data will be used to update any personal data the police currently hold about you
- Other data sources such as British Transport Police(Opens in a new window), the Royal Military Police(Opens in a new window), the Ministry of Defence Police(Opens in a new window). Searches are made of an internal database which lists the nominal details of those upon whom these departments hold data. Where a match occurs the information will be shared to clarify whether that data is information held about you.
- Disclosure Scotland – if you have spent any time living in Scotland, your details may be referred to Disclosure Scotland
- Customer satisfaction surveys-– the DBS may conduct customer satisfaction surveys and may employ a specialised organisation to conduct the survey on their behalf. The data used includes: name, address, age, gender, telephone number and email address. Customer Satisfaction packs are issued directly from DBS to persons referred for barring consideration, no information is passed to any third party
- United Kingdom Central Authority - for information exchange with other EU countries in accordance with the decision made by the council of The European Union
- the Child Exploitation Online Protection Centre (CEOP) who are an affiliate of the Serious Organised Crime Agency (SOCA)
- Data may be shared with Keepers of Registers and Registered Bodies etc as defined in the Safeguarding Vulnerable Groups Act and Protection of Freedoms Act or secondary legislation

Keepers of Registers

Care Council for Wales (CCW);
Education and Training Inspectorate (NI) (ETI);
General Chiropractic Council (GCC);
General Dental Council (GDC);
General Medical Council (GMC);
General Optical Council (GOptC);
General Osteopathic Council (GOstC;
General Teaching Council Northern Ireland (GTCNI);
General Teaching Council Wales (GTCW);
Health and Care Professions Council (HPC);
Northern Ireland Social Care Council

Supervisory Authorities

Care and Social Services Inspectorate Wales (CSSIW);
Care Quality Commission (CQC);
Charity Commission (CC);
Charity Commission for Northern Ireland (CCNI);
Children's Health and Social Services Directorate, Wales (CHSSD);
Estyn;
Health Inspectorate Wales (HIW);
Office of the Public Guardian (OPG);
Ofsted;
Regulation and Quality Improvement Authority (RQIA);
Teaching Agency (TA);

(NISCC);
Nursing and Midwifery Council (NMC);
Pharmaceutical Society of Northern Ireland (PSNI);
Royal Pharmaceutical Society of Great Britain (RPSoGB);

Other partners we may share information with

In certain circumstances we will share information with the police and probation services. We may also share information with organisations or individuals you have provided consent for. This will only occur where our customers choose to allow the sharing to take place.

Any member of staff that has access to your data will be thoroughly checked by a governmental security unit. All our staff are data protection trained and are aware of their responsibilities under the Act.

We conduct regular compliance checks on all DBS departments and systems. All checks are to the standard set out by the Information Commissioners Office. In addition continual security checks on our IT systems are undertaken.

Reasons for requesting personal data

The data contained within the DBS is often sensitive. It may be that it contains details of offences or convictions. For this reason we must be sure of the identity of an applicant. We have a duty to make certain that any data disclosed is both accurate and relevant.

It is important that we conduct a complete and accurate check of each applicant. Your data is requested for the sole reason that it is necessary to the DBS Disclosure and Barring functions.

What data is necessary for a Disclosure application?

The form asks only for data that is necessary. Further details can be found in the Disclosure guidance notes.

Please note - the DBS will access previous applications to assist in the checking process.

Why does the DBS require personal details of counter signatories?

A key part in the Disclosure checking process is that played by a counter signatory. We must make sure that they do not have a background that would make them

unsuitable to receive your data. The data requested will allow us to check identity and carry out an enhanced check.

Retention of data

The DBS will ensure that data is not held for longer than is necessary for the purpose. In establishing retention and archiving periods, the DBS will make provision for repeat disclosure applications, complaints and legal requirements.

Storage of data

Your data is held in secure computer files, which have restricted access. We have approved measures in place to stop unlawful access and disclosure.

Individual rights

An individual has a number of rights under the Data Protection Act 1998 which include:

- to ask us to amend any data if it is incorrect
- to ask us not to process information used for the disclosure certificate if it would cause substantial unwarranted damage or distress
- to ask for non automated decisions to be made regarding their data
- compensation for damage caused through a data protection breach
- access to the data we hold. Please note - if your disclosure application has been inactive for four or more years the DBS will no longer hold copies of application forms and incoming/outgoing documents. Application data such as system notes will still be available
- the right to stop unsolicited marketing

Transfer outside the European Economic Area

If you have recently lived in the Channel Islands or the Isle of Man, it is likely that your data will be passed to police forces in the that area. If your data needs to be transferred there or anywhere else, in accordance with the council of The European Union's decision we will make sure that an adequate level of protection is in place.

Notification of changes

If we decide to change our privacy policy, we will add a new version to our website.