Our Christian faith emphasises the value and worth of every individual
with their own distinctive character, gifts and abilities.

Christ's command to 'Love one another' calls us to respect and help other people.
This provides the foundation for our school and all we aim to achieve.

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

DBS SECURE STORAGE, HANDLING, USE, RETENTION & DISPOSAL OF DISCLOSURE INFORMATION POLICY

The Policy

At Holy Trinity C of E Primary School we adopt the current Royal Borough of Windsor and Maidenhead's Professional Capability Procedure – Teaching Staff in Schools.

The Governing Body first approved the adoption of this RBWM policy on 23rd October 2025

Signed: Chair of Governors

Signed: Head Teacher

Covers:

- **Storage and access**
- **Handling and usage**
- **Retention**
- **Disposal**
- **Umbrella body**

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

DBS SECURE STORAGE, HANDLING, USE, RETENTION & DISPOSAL OF DISCLOSURE INFORMATION POLICY

1. Introduction

This Policy explains the Royal Borough of Windsor and Maidenhead's position on the secure storage, handling, use, retention & disposal of disclosure information.

The Royal Borough of Windsor and Maidenhead ("we", "us" and "our") refers to the Registered Body who is responsible for the applications processed through this website, whose office is Town Hall, St Ives Road, Maidenhead, SL6 1RF.

We reserve the right to revise this policy or any part of them from time to time, so you should review these terms periodically for changes.

General Principles

As an organisation using the services of the Disclosure and Barring Service, Disclosure Scotland and Access NI we agree to comply fully with their respective Codes of Practice, in particular with regard to the correct handling, use, storage, retention and disposal of disclosures and disclosure information.

We also comply fully with our obligations under data protection legislation, including the Data Protection Act, the General Data Protection Regulation and all other relevant legislation relating to the safe handling, use, storage, retention and disposal of disclosure information.

2. Arrangements

Handling

In accordance with section 124 of the Police Act 1997, disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom disclosures or disclosure information has been revealed and we recognise that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Access

System access is only granted to authorised personnel, which ensures that access to disclosure information is only available to individuals who are involved in the recruitment decision. Access is only available with username and password protection to prevent unauthorised access or modification.

Scanning/copying of DBS information

Where an applicant presents a previously completed disclosure certificate and supporting details, for example to access the DBS Update Service, we shall only scan/copy a disclosure certificate with the written permission of the applicant. To scan/copy a disclosure certificate that contains information that we are not entitled to see - either children's barring information or adult barring information - is not permitted and could constitute a breach of the applicant's rights under data protection legislation.

Printing of disclosure information

Communication of disclosure result information (verbal, written, or by email etc.) must only be between individuals who are involved in the recruitment decision or are entitled to access disclosure information as a part of their ordinary duties.

DBS result information must be printed no more than once and is only available with username and password protection to prevent unauthorised access or modification.

Readable copies may be printed for the purpose of presenting them to relevant industry regulatory inspectors at the time of an inspection. Where applicable this may include, for example, auditors/inspectors from the Department for Education (DfE), Ofsted, Care Quality Commission (CQC), Care Inspectorate Wales (CIW), Financial Standards Authority (FSA)/Financial Conduct Authority (FCA), Law Society, Solicitors Regulation Authority.

Forwarding of electronic disclosure information
Forwarding of disclosure result information is not permitted on the system. Documents may not be saved into any format outside of the online system and cannot be stored separately electronically, emailed or distributed.

Usage
Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Loss of Documents
If disclosure information is lost, such loss must be reported to Atlantic Data Ltd or the registered body countersigning the application, stating what has been lost, how, in what format and by whom.

Failure to comply with this policy could result in:
- a non-compliance notice being issued and a requirement to remedy and provide evidence of the remedial action within 14 days.
- suspension of the user(s) from the account.
- suspension or termination of the online account.

Storage
Disclosure result information, whether a disclosure certificate, electronic result information, printed result information or scanned/copied result information must be handled in accordance of the relevant Codes of Practice. We ensure that every user is provided with a policy statement on the secure storage, handling, use, retention and disposal of disclosure information, as well as full access to the DBS Code of Practice.

Retention
We do not keep disclosure information for any longer than is necessary. Original and scanned/copied disclosure certificates will be kept for a maximum of 6 months to allow for the recruitment decision to take place and for the consideration and resolution of any disputes or complaints.

If circumstances dictate that is necessary to keep disclosure information for longer than 6 months, this will be for a period of no longer than 12 months. This must also be with the prior agreement of the applicant. We will also consult the DBS and will give full consideration to the data protection and human rights of the individual before doing so.

Original certificates or printed disclosure result information may be retained in exception to the 6-month retention period in circumstances where an industry regulator has a statutory or legal right to audit disclosure result of relevant personnel. Such examples include:
- Adult care home or domiciliary care services regulated by the CQC.
- Schools or nurseries regulated by DfE and/or Ofsted.
- An organisation working with or within an NHS Trust or Hospital in compliance with the NHS employer check standards.

DBS application information
We do not keep applicant data for any longer than is necessary. The personal data forming a basic record of an application will be retained as a record of the application for up to seven years. This includes the applicant’s name, address, date of birth, and contact details. Supporting information provided as part of the disclosure application, such as identity documents, previous names and addresses will be purged from the system after one year.

Disposal:
Manual Disposal Methods - once the retention period has elapsed, we will ensure that any disclosure information is destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

Shredding is conducted at a ‘Level 4 (DIN 4)’ standard. (en15713)

We will not keep any photocopy or other image of the disclosure or any copy or representation of the contents of a disclosure. No electronic copies of disclosure certificates will be retained in any electronic format.

DBS-related data in RBWM is stored either on hard disks within RBWM Data Centres, or stored in Microsoft Cloud storage services.

Data Stored in RBWM Data Centres
Data deletion on physical storage devices
•If a disk drive used for storage suffers a hardware failure, it is securely destroyed by physically shredding the device to ensure that the data cannot be recovered by any means.

Data Stored in Microsoft Data Centres
Microsoft is governed by strict standards and follows specific processes for removing cloud customer data from systems under our control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware.
Data retention
In our Online Services Terms, Microsoft contractually commits to specific processes when a customer leaves a cloud service or the subscription expires. This includes deleting customer data from systems under our control and:
•If you terminate a cloud subscription or it expires, Microsoft will store your customer data in a limited-function account for 90 days (the “retention period”) to give you time to extract the data or renew your subscription.
•After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period.

Data deletion on physical storage devices
•If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure that the data cannot be recovered by any means.
•When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

Acting as an umbrella body
Before acting as an umbrella body (an umbrella body being a registered body which countersigns applications and receives disclosure result information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that our clients will store, handle, use, retain and dispose of disclosure information in full compliance with the relevant Codes of Practice and in full accordance with this Policy.

We will also ensure that any organisation or individual, at whose request applications for disclosures certificates are countersigned, has such a written policy and, if necessary, will provide a sample policy for that body or individual to use or adapt for this purpose.

Further advice
Further advice can be obtained from HR by contacting HR.operations@rbwm.gov.uk or calling 01628 796794.