

Bishop Lonsdale Church of England

Primary School & Nursery

**Handling of Personal Data Policy**

**A Derby Diocesan Academy Trust Policy**

Approved April 2020

Review April 2021

Signed……………………………………………Chair of Governors

1. **The Purpose of this Policy**

The Derby Diocesan Academy Trust (DDAT), and its staff will do everything within their power to ensure the safety and security of any material of a personal and sensitive nature, regardless of whether it is held on paper or in electronic format.

A breach may arise from a theft, a deliberate attack on the academy/Trust systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure.

It is the responsibility of all members of the Trust to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

* have permission to access the data; and/or
* need to have access to that data

Data breaches can have serious effects on individuals and the Trust. It could bring the Trust into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the academy, The Trust and the individuals involved.

At DDAT, anyone who has access to personal data must know, understand and adhere to this policy.

1. **Policy Statement**

The Trust will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see Privacy Notice section below)

1. **Personal Data**

The Trust will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

* Personal information about members of the academy community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship, contact details, health records, disciplinary records
* Curricular / academic data e.g. class lists, pupil progress records, reports, references
* Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
* Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

1. **Responsibilities**

The Trust’s Data Protection Officer is the Academy’s Business Manager. This person will keep up to date with current legislation and guidance and will determine and take responsibility for the Trust’s information risk assessments (see section 8)

The Data Protection Officer will identify the varioustypes of data being held (e.g. pupil information / staff information / assessment data etc) and who has access to the information.

The Data Protection Officer will manage and address risks to the information and will understand:

* what information is held, for how long and for what purpose,
* how information is amended or added to over time, and
* who has access to protected data and why.

Everyone in the Trust has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a governor.

The Data Protection Officer will inform the Headteacher of the relevant academy and Head of the Multi Academy Trust of any concerns over data protection.

1. **Registration**

All academies within the Trust and the Trust itself are registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

**6.0 Information to Parents/Carers – “The Privacy Notice”**

In order to comply with the fair processing requirements of the Data Protection act, the Trust will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. DfE, Multi Academy Trust etc.) to whom it may be passed. This privacy notice will be made available to parents / carers on the website and via the school newsletter. Parents / carers of young people who are new to the school will be provided with the privacy notice on joining the academy.

**7.0 Training and Awareness**

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

* Induction training for new staff
* Staff meetings / briefings / Inset
* Day to day support and guidance from Data Protection Officer

**8.0 Risk Assessments**

Information risk assessments will be carried out by the Data Protection Officer in each Academy to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

* Recognising the risks that are present;
* Judging the level of the risks (both the likelihood and consequences); and
* Prioritising the risks.

Risk assessments are an on-going process and should result in the completion of an Information Risk Actions Form (see Template 1)

**9.0 Impact Levels and Protective Marking**

The Trust will ensure that all academy staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered ‘unclassified’. The term ‘UNCLASSIFIED’ or ‘NON‘ or ‘NOT PROTECTIVELY MARKED’ may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone’s reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. “Securely delete or shred this information when you have finished using it”.

|  |  |  |
| --- | --- | --- |
| **Government Protective Marking Scheme label** | **Impact Level (IL)** | **Applies to schools?** |
| NOT PROTECTIVELY MARKED | 0 | Will apply in schools |
| PROTECT | 1 or 2 |
| RESTRICTED | 3 |
| CONFIDENTIAL | 4 | Unlikely to apply in schools |
| HIGHLY CONFIDENTIAL | 5 |
| TOP SECRET | 6 |

**10.0 Secure Storage of and Access to Data**

The Trust will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on Trust or academy equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

* All the data must be encrypted and password protected,
* the device must be password protected
* the device must offer approved virus and malware checking software, and
* the data must be securely deleted from the device, in line with Trust policy (see section 12) once it has been transferred or its use is complete.

The Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups

The Trust has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see the ICO advice on cloud based storage [http://ico.org.uk/for\_organisations/guidance\_index/~/media/documents/library/Data\_Protection/Practical\_application/cloud\_computing\_guidance\_for\_organisations.ashx](about:blank))

As a Data Controller, the Trust is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The Trust recognises that under Section 7 of the Data Protection Act, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the Data Controller in connection with the data subject. Data subjects have the right to know: if the Data Controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

**11.0 Secure Transfer of Data and Access out of the Academy / Trust**

The Trust recognises that personal data may be accessed by users out of the Trust / academy, or transferred to other agencies. In these circumstances:

* Users may not remove or copy sensitive or restricted or protected personal data from the Trust/academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see section 10)
* Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
* When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
* If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
* Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
* Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the Trust in this event. *(nb: to carry encrypted material is illegal in some countries)*

**12.0 Disposal of Data**

The Trust will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data. Guidance for the deletion of data from electronic devices can be found at: [http://ico.org.uk/for\_the\_public/topic\_specific\_guides/online/deleting\_your\_data](about:blank)

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

**13.0 Audit Logging / Reporting / Incident Handling**

It is good practice, as recommended in the “Data Handling Procedures in Government” document that the activities of data users, in respect of electronically held personal data, should be logged and these logs will be monitored by responsible the Data Controller.

Where audit logs exist these will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The Trust has a policy for reporting, managing and recovering from information risk incidents and all incidents will be reported to the Headteacher and the Head of the Multi Academy Trust.

All significant data protection incidents must be reported through the Data Protection Officer to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

**14.0 Use of Technologies and Protective Marking**

The following provides a useful guide:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **The information** | **The technology** | **Notes on Protect Markings (Impact Level)** |
| **School life and events** | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events | Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| **Learning and achievement** | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child’s learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the PROTECT (Impact Level 2) category.  There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way. |
| **Messages and alerts** | Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging are commonly used by schools to contact and keep parents informed.  Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context. | Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information.  General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

Additional Issues / Documents related to Personal Data Handling in Schools:

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

* For all pupils in academies under 18, they must obtain the written consent of a parent before they take and process their child’s biometric data.
* They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
* They must provide alternative means for accessing services where a parent or pupil has refused consent.

New advice to academies will make clear that they will no longer be able to use pupils’ biometric data without parental consent. The advice came into effect from September 2013. Academies may consider any changes in legislation when reviewing their Personal Data Handling policy. Academies should consider incorporating the parental permission procedures into existing parental forms (e.g. AUP / Digital & Video Images permission form – see template in e-Safety Policy).

**Use of Cloud Services**

Many academies now use cloud hosted services. When considering switching from locally-hosted services to cloud-hosted services academies need to consider a number of issues.

The academy is ultimately responsible for the contract with the provider of the system, so check the terms and conditions carefully; below is a list of questions that you may want to consider when selecting a cloud services provider; indeed you may want to contact any potential provider and ask them for responses to each of the following:

* How often is the data backed up?
* Does the service provider have a clear process for you to recover data?
* Who owns the data that you store on the platform?
* How does the service provider protect your privacy?
* Who has access to the data?
* Is personal information shared with anyone else? Look out for opt in/opt out features
* Does the service provider share contact details with third party advertisers? Or serve users with ads?
* What steps does the service provider take to ensure that your information is secure?

Is encryption used? Is https used as default or is there an option to use this? Two step verification?

* How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware
* How reliable is the system? Look out for availability guarantees.
* What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

A useful summary of these issues in a document that has been written with the support of Google and Microsoft: [http://www.swgfl.org.uk/News/Content/News-Articles/Cloud-based-products-and-services](about:blank)

The document focusses on Google Apps for Education and Microsoft 365, but poses important considerations if a school is considering services from another provider.

**Parental permission for use of cloud hosted services**

Academies that use cloud hosting services (eg.Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - [http://www.google.com/apps/intl/en/terms/education\_terms.html](about:blank) requires a school to obtain ‘verifiable parental consent’. Normally, academies will incorporate this into their standard acceptable use consent forms sent to parents each year (see template in the Academy e-Safety policy)

For further information see the ICO Guidance: [http://www.ico.org.uk/for\_organisations/guidance\_index/~/media/documents/library/Data\_Protection/Practical\_application/cloud\_computing\_guidance\_for\_organisations.ashx](about:blank)

**RISK ASSESSMENT - HANDLING OF PERSONAL DATA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Information Held** | **Information User** | **Protective Marking (Impact Level)** | **Likelihood** | **Overall risk level (low, medium, high)** | **Action(s) to minimise risk** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |