DIXONS ACADEMIES TRUST

# Data Classification, Handling and Disposal Policy

Responsibility for Review: Executive Director, Dixons Academies Trust
Date of Last Review: September 2020

# Contents

## 1.0 Policy statement

The purpose of this policy is to define a system of categorising information in relation to its sensitivity and confidentiality, and to define associated rules for the handling of each category of information to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

The policy aims to:

- protect information from accidental or deliberate compromise, which may lead to damage, and / or be a criminal offence
- help to meet legal, ethical and statutory obligations
- protect the interests of all those who have dealings with the Trust and about whom it may hold information (including its staff, students, alumni, funders, collaborators, business partners, supporters etc.)
- promote good practice in relation to information handling

## 2.0 Scope and purpose

This policy covers all information held by and on behalf of Dixons Academies Trust and the handling rules shall apply to members of the Trust and to third parties handling Trust information. Where the Trust holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply.

## 3.0 Relationship with existing policies

This policy forms part of the Trust's Information Security Policies. It should be read in conjunction with the "Information Systems Security Manual and Guidelines" and all supporting policies.

## 4.0 Policy Statement

All members of Dixons Academies Trust and third parties who handle information on behalf of Dixons Academies Trust have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the Trust. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

Automatic technical controls may be implemented to assist users in complying with these controls, but where technical measures are not implemented users are responsible for complying with this policy.

## 5.0 Policy

5.1 All information held by or on behalf of Dixons Academies Trust shall be categorised according to the Information Classification (Annex 1). The categorisation shall be determined by the originator of the information and all information falling into the classified categories shall be marked as such.

5.2 Information shall be handled in accordance with the Information Handling Rules (Annex 2) and where information falls within more than one category, the higher level of protection shall apply in each case.

5.3 Where a third party will be responsible for handling information on behalf of Dixons Academies Trust, the third party shall be required by contract to adhere to this policy prior to the sharing of that information.

5.4 Where the Trust holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information.

## 6.0 Responsibilities

6.1 The Data Protection Officer shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.

6.2 It shall be the responsibility of every individual handling information covered by this policy, to mark classified material as such, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a line manager, or the GDPR Champion where they are unsure as to how to label or handle information.

6.3 All members of the Trust shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the Data Protection Officer.

## 7.0 Compliance

7.1 Breaches of this policy may be treated as a disciplinary matter dealt with under the Trust's staff disciplinary policies or the Student Code of Conduct as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

## Annex 1 - Information classification

| Level | Definition | Protection required | Examples |
|---|---|---|---|
| **Personal** | Non-business data, for personal use only | No Trust requirement | |
| **Public** | Trust information that is specifically prepared and approved for public consumption.<br>This is information which does not require protection and is considered 'open' or 'unclassified' and which may be seen by anyone whether directly linked with the Trust or not. | Key security requirement: **Availability**<br>This information should be accessible to the Trust whilst it is required for business purposes<br>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it? | Prospectus, programme and course information<br>Key Information Sets<br>Press releases (not under embargo)<br>Open content on the Trust website<br>Fliers and publicity leaflets<br>Published information released under the<br>Freedom of Information Act responses<br>Policies once they are approved<br>Annual Report and Financial Statements |
| **Restricted** | Non-Confidential information where dissemination is restricted in some way e.g. to members of the Trust, partners, suppliers or affiliates. Access to this information enhances Trust operations by facilitating communication and collaboration between staff, students and external partners, but access is restricted and governed by appropriate policies or contracts<br>The documents may be restricted to the Trust, or to a group in it, or to a group in the Trust and an external partner.<br>Note that documents marked 'Restricted' might lose this marking over time. | Key security requirements: **Availability**<br>This information should be accessible to the Trust whilst it is required for business purposes<br>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it? | Some committee minutes<br>Departmental intranets<br>Trust timetable<br>On-line directory of contact details<br>Teaching materials<br>Procurement documents<br>Internal briefing papers |

| | | | |
|---|---|---|---|
| **Confidential** | Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged, or under embargo before being released at a particular time.<br>**This data has the potential to cause a negative impact on individuals' or the Trust's interests (but not falling into Highly Confidential).**<br>It also includes information in a form that could not be disclosed under Freedom of Information legislation.<br>Covers data about an individual, and data about the institution.<br>This information, if compromised, could:<br>• cause damage or distress to individuals<br>• breach undertakings to maintain the confidence of information provided by third parties<br>• breach statutory restrictions on the use or disclosure of information or lead to a fine, e.g. for a breach of the Data Protection Act or Competition Law<br>• breach contractual agreements<br>• breach a duty of confidentiality or care<br>• cause financial loss or loss of earning potential to the Trust<br>• disadvantage the Trust in commercial or policy negotiations with others<br>• prejudice the investigation or facilitate the commission of crime<br>• undermine the proper management of the Trust and its operations | Key security requirements:<br>**Confidentiality and integrity**<br>This information requires security measures, controlled and limited access and protection from corruption<br>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it? | Data contains private information about living individuals and it is possible to identify those individuals *e.g. individual's salaries, student assessment marks*<br>• Non-public data relates to business activity and has potential to affect financial interests and / or elements of the Trust's reputation *e.g. tender bids prior to award of contract, exam questions prior to use*<br>• Non-public information that facilitates the protection of the Trust's assets in general *e.g. access codes for lower risk areas*<br>Internal Reports<br>Commercial Contract<br>Data relating to living individuals, whether employees of this Trust or not.<br>Data that is commercially sensitive to a project or a company providing research funds. |
| **Highly confidential** | Has the potential to cause serious damage or distress to individuals or serious damage to the Trust's interests if disclosed inappropriately<br>*Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria*<br>• Data contains highly sensitive private information about living individuals and it is possible to identify those individuals *e.g. Medical records, serious disciplinary matters.*<br>Non-public data relates to business activity and has potential to seriously affect commercial interests and / or the Trust's corporate reputation e.g. REF strategy<br>• Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets *e.g. access codes for higher risk areas, Trust network passwords.* | Key security requirements:<br>**Confidentiality and integrity**<br>This information requires significant security measures, strictly controlled and limited access and protection from corruption<br>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it? | Student personal details<br>Staff personal details<br>Financial transactions<br>Research data<br>*Medical records*<br>Patient-level research data<br>Serious disciplinary matters<br>Corporate reputation e.g. *REF strategy access codes for higher risk areas*<br>*Trust network passwords*<br>Papers relating to possible redundancies<br>Patient-level research data |

Information may also be marked with a descriptor, which identifies the reason why the classification is applied. The expiry date for the current level may also be given. For example:

- Confidential - personal
- Confidential - commercially sensitive
- Confidential - exams - expires 1 July 2020 and becomes public

Qualifying descriptors may also be used to incorporate/map to protective markings from other classification schemes, where staff are working with external partners, data and schemes (e.g. the Government Protective Marking Scheme). For example: Confidential - GPMS Secret.

## Annex 2 - Data handling

| Class | Description | Storage | Dissemination and access | Exchange and collaboration | Disposal |
|---|---|---|---|---|---|
| **Public** | Trust information that can be seen by anyone. | Electronic information should be stored using Dixon's Academies Trust provided<br>IT facilities to ensure appropriate management, backup and access. | Information can be shared via the web without requiring a Dixon's Academies Trust username.<br>Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition<br>May be accessed remotely and via portable and mobile devices without encryption. | Information can be exchanged via email or file sharing without needing encryption. | Electronic information should be deleted using normal file deletion processes in accordance with any retention schedule.<br>Printed copy should be disposed of via the Trust paper recycling scheme and in accordance with any retention schedule. |
| **Restricted** | Non-confidential information where dissemination is restricted in some way e.g. information restricted to members of the<br>Trust, a committee, project or partnership. | Electronic and paper-based Information must be stored using Dixon's Academies Trust provided facilities. | Information can be shared via the web, but the user must provide Dixon's Academies Trust authentication, or a federated authentication<br>Electronic and hard copy information can be circulated on a need-to-know basis to Trust members subject to applicable laws (e.g. copyright) and Trust Regulations<br>May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption. | Information can be sent in unencrypted format via email.<br>Information can be shared using Dixon's Academies Trust IT facilities e.g. OneDrive, SharePoint, shared file store.<br>Information can be printed and circulated via the Trust internal mail service. | Electronic equipment holding this information must be disposed of using the Trust secure IT waste disposal service and in accordance with any retention schedule.<br>Printed copy should be disposed of via the Trust confidential waste scheme and in accordance with any retention schedule. |

| Class | Description | Storage | Dissemination and access | Exchange and collaboration | Disposal |
|---|---|---|---|---|---|
| **Confidential** | Information which is sensitive in some way because it may be personal data, commercial or legal information, or be under embargo prior to wider release.<br>Includes data about individuals, and data about the institution.<br>May also include data provided to the Trust by other organisations e.g. research datasets | Information must be stored using Dixon's Academies Trust IT facilities. Portable devices must have full disk encryption.<br>Unencrypted removable media<br>(e.g. USB sticks) must not be used.<br>Encrypted removable media are not permitted without undertaking evaluation of other options.<br>Storage on Personally owned (e.g. home) computer is NOT permitted. | Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews.<br>Some types of confidential information may be shared with authorised users via Dixon's Academies Trust IT facilities, including remote access, subject to Dixon's Academies Trust authentication.<br>For web access encryption must be used.<br>**Confidential data must not be extracted from Trust IT systems and stored on local IT systems.**<br>If a portable device (e.g. a laptop, tablet or phone) is used to access Trust confidential information, the device must be encrypted and require a password or PIN to access | The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed, and an appropriate method selected.<br>Approved data exchange methods are available from Digital Services.<br>**Confidential data must be encrypted**<br>Exchange must be conducted using Dixon's Academies Trust provided facilities.<br>Duplicate copies of confidential information must be avoided. Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used.<br>Paper and electronic copies must be marked 'Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used. Electronic equipment holding this information must be disposed of using the Trust secure IT waste disposal service and in accordance with any retention schedule. | Electronic equipment holding this information must be disposed of using the Trust secure IT waste disposal service and in accordance with any retention schedule.<br>Printed copy should be disposed of in accordance with any retention schedule via the Trust confidential waste scheme or departmental shredding facilities.<br>Large accumulations of data should not be downloaded or copied. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Printed copy should be disposed of in accordance with any retention schedule via the Trust confidential waste scheme or departmental shredding facilities.<br>Large accumulations of data should not be downloaded or copied. | |
| **Highly Confidential** | Information which is sensitive and has the potential to cause serious damage or distress to individuals or serious damage to the Trust's interests if disclosed inappropriately.<br>Data contains highly sensitive private information about living individuals and it is possible to identify those individuals e.g. Medical records, serious disciplinary matters. | Information must be stored using Dixon's Academies Trust IT facilities. Portable devices must have full disk encryption.<br>Unencrypted removable media<br>(e.g. USB sticks) must not be used.<br>Encrypted removable media are not permitted without undertaking evaluation of other options.<br>Storage on Personally owned (e.g. home) computer is NOT permitted. | Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews.<br>Some types of confidential information may be shared with authorised users via Dixon's Academies Trust IT facilities, including remote access, subject to Dixon's Academies Trust authentication.<br>For web access encryption must be used.<br>**Confidential data must not be extracted from Trust IT systems and stored on local IT systems.**<br>If a portable device (e.g. a laptop, tablet or phone) is used to access Trust confidential information, the device must be encrypted and require a password or PIN to access. | The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed, and an appropriate method selected.<br>Approved data exchange methods are available from Digital Services.<br>**Confidential data must be encrypted prior to exchange.**<br>Exchange must be conducted using Dixon's Academies Trust provided facilities.<br>Duplicate copies of confidential information must be avoided. Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used.<br>Paper and electronic copies must be marked 'Highly Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used. | Electronic equipment holding this information must be disposed of using the Trust secure IT waste disposal service and in accordance with any retention schedule.<br>Printed copy should be disposed of in accordance with any retention schedule via the Trust confidential waste scheme or departmental shredding facilities.<br>Large accumulations of data should not be downloaded or copied. |