achieving for children

Information Classification and Protective Marking Policy

Introduction

This policy details Achieving for Children's approach to information classification and protective marking.

Background and context to the Policy

All users and custodians of sensitive data have a responsibility to be able to identify and protect it. Failure to carry out this responsibility can lead to sensitive information being lost and could result in a breach of the Data Protection Act (DPA).

Achieving for Children adopted the common Information Classification and Protective Marking scheme shown below in order to help users and custodians of sensitive information to carry out these responsibilities effectively. The mapping of this information Classification and Protective marking scheme used by other public bodies, government agencies and partner organisations is shown at the end of this policy.

The classification system set out in the Information Classification and Protective Marking Policy is based on definitions of personal and sensitive data as stated in the DPA. An explanation of personal and sensitive data is included along with examples of each in Table 1 below.

	Personal	**Sensitive**
Explanation	Personal information is information that relates to and can identify a living individual, and is about them. This includes opinions about them made by others. Data can also be considered as personal if the data controller is in possession of further information that when combined identifies an individual data subject.	The DPA specifically defines sensitive personal data as information relating to their: 1. Racial or ethnic origin of a person (the data subject); 2. Political opinions; 3. Religious beliefs or other beliefs of a similar nature; 4. Trade union membership; 5. Physical or mental health or condition; 6. Sexual life; 7. Criminal record details including alleged offences

Examples	• Name • Address • Postcode • Email • Telephone numbers • Driving license number	• Bank, financial or credit card details • Mothers maiden name • National insurance number • Employment records • Health records • School attendance or records • Data relating to social services including child protection and housing • DNA or fingerprints

Aims of the Information Classification and Protective Marking Policy

- To inform employees as to how they should mark documents and communications to ensure they are appropriately processed.

Objectives of the Information Classification and Protective Marking Policy

To:

- provide information to practitioners;
- protect information we consider sensitive or in need of protection
- demonstrate a consistent and, measured approach to information security management and governance; and
- enable Achieving for Children to communicate with our stakeholder to deliver the best possible service to our residents.

Implementing the Information Classification and Protective Marking Policy

Classifying Information

Achieving for Children will adopt the following information classifications based on the potential impact which could result to an individual(s) or organisation(s) should the information be lost or otherwise compromised:

- Unclassified: Non-sensitive information, including any information which is subject to disclosure under the terms of the Freedom of Information Act.
- Classified
    - Protect: Sensitive Personal Information which could have a low to medium impact if the information is compromised. For example, this would include:
        - the potential for embarrassment or harm to an individual, or
        - loss of trust and confidence in the organisation.
    - Restricted: Sensitive Personal Information which could have a high impact if the information is compromised. For example, this would include:
        - risk of significant harm to an individual, or

- result in an individual potentially posing a significant risk to someone else.

If a compromise to personal and/or sensitive personal data could put an individual(s) or organisation(s) at risk of harm or distress it should be considered Sensitive Personal Information.

All Sensitive Personal Information by default should be classified as Protect unless it is felt that a compromise to the confidentiality of this information could put individuals at risk of significant harm of distress. If this is the case it should be classified as Restricted, the higher of the two classification types.

The key difference between the Protect and Restricted classification types, hinges on the word significant. A professional judgement needs to be made based on best intentions, when classifying Sensitive Personal Information, whether a compromise to the information could put an individual(s) or organisation (s) at risk of significant harm or distress, as opposed to at risk of harm or distress.

Other public bodies, government agencies and partner organisations use alternative classifications. A mapping of the most commonly used classifications is provided in Appendix 2.

Marking Information

Information which is classified as Protect or Restricted must be marked (e.g. in document filenames or email subject lines) to make sure that recipients are clear about the status of the information. It is not necessary to mark unclassified information. Examples of information types and their appropriate classification are included in Appendix 1.

Non-compliance

Non-compliance with the Information Classification and Protective Marking Policy may lead to disciplinary procedures as set out in the Disciplinary Code of Conduct. Any breach of the Information Classification and Protective Marking Policy or any associated documents will be dealt with in accordance with those procedures. Staff must wherever possible classify and mark information appropriately.

Roles and responsibilities for implementing, monitoring and reviewing

Information Governance Lead	• Providing direction in establishing, promoting and implementing Information Classification and Protective Marking Policy. • Following up and where appropriate escalating to the Information Governance Group cases where information has been incorrectly classified and

	marked to help avoid similar occurrences in the future.
Line Managers	• Support their staff in meeting the requirements of the Information Classification and Protective Marking Policy by ensuring that they are aware of: o their responsibility for classifying and marking information; and o where to get advice on how to correctly classify and mark information. • Reporting cases where information has been incorrectly classified and marked to the Information Governance Lead. • Ensuring staff have skills, time and capacity to undertake appropriate marking.
All employees	• Classifying information they are responsible for according to the Information Classification and Protective Marking Policy. • Seeking further advice if they are uncertain how to proceed. • Alerting their line manager if they discover an information source that has not been classified and marked or has been incorrectly classified and marked.

This policy will be reviewed after a period of two years by Achieving for Children to judge its effectiveness, or updated sooner in accordance with changes in legislation.

Appendix 1

Examples of information classification

Examples of the types of information that fall into the UNCLASSIFIED (no impact), PROTECT (low to medium impact) and RESTRICTED (high impact) classifications are shown below.

UNCLASSIFIED (no impact)

- Policies and procedures
- Documents or other information available in the public domain or disclosable under the terms of the Freedom of Information Act
- Names and contact details of specific employees, citizens or businesses that are in the public domain or which an individual has authorised
- Property addresses where it does not identify the individual owner or residents
- Open data and any other information made publicly available under appropriate Government Codes of Practice
- Anonymised or depersonalised data where personal data cannot be identified or traced

PROTECT (low to medium impact)

- Personal information relating to any customer or employee for which we have a duty to keep the data confidential or withhold as personal data under a Freedom of Information request. This would include information such as name, address and contact details, together with other personal data such as VAT number, National Insurance (NI) number, bank details, and financial assessments
- Employee records / case files or customer records / case files, e.g. service user care plan, employee appraisal
- Any other documents containing information for which we have a duty to protect privacy
- Policies, procedures or other business documents which are in draft for and which have not yet been released into the public domain and would not be released to the public in draft form
- Exempt Committee papers excluded from public disclosure
- Information that does not contain personal data but should not be made public for copyright reasons
- The employees directory with contact numbers, address, position, where the information is not already publicly available
- Documents containing commercial information which is not subject to release under the terms of the Freedom of Information Act. This would include tender submissions before contract award and documents containing commercially sensitive information which should not be disclosed

RESTRICTED (high impact)

- An individual's complete set of social care paper files or an electronic record equivalent
- NHS Patient Identifiable Data
- Legal court bundle for a child protection case
- A complete employee record / case file, especially if containing health or other sensitive personal data
- A complete customer record / case file, especially if containing health or other sensitive personal data
- Documents and communication of a serious case review
- A complete individual's or business case file that involves court proceedings or investigations leading to prosecution.
- Information gathered for surveillance purposes under the Regulation of Investigatory Powers Act (RIPA)
- Contact details and address of a high risk vulnerable child or adult (e.g. an individual who is in a refuge or otherwise at risk)
- Mental health assessments
- Partial customer, social care, employee or business records for a volume of more than 100 individuals, where the individuals can be identified
- Some sensitive property plans, e.g. plans and maps of properties that have security implications or external property plans held by Fire & Rescue or Emergency / Resilience Planning team

Other information may also be classified as RESTRICTED (high impact) based on the volume of data. This would include:

- Business systems and databases containing personal data
- Business systems and databases containing information which is commercially sensitive, or relates to investigation or legal proceedings
- Complete email database / account for a user with a high risk employees role (e.g. social workers)
- Extracts taken out of business systems and databases containing more than 100 records containing personal data or information which is commercially sensitive or relates to investigations or legal proceedings
- Boxes of paper records in transit from offices or during office moves
- The equivalent electronic records in transit (e.g. output from scanning or conversion, volumes of data sharing or processing)

Appendix 2

Mapping Achieving for Children, RBK and LBS information classifications to those used by other public bodies, government agencies and partner organisations.

Other organisations use different marking schemes. The table below shows how to map these to the Achieving for Children, RBK and LBS information classifications.

Achieving for Children, RBK and LBS classifications	NHS classifications	Central Government classifications
UNCLASSIFIED (no impact)	NHS Unclassified	OFFICIAL
PROTECT (low to medium impact)	NHS Protect	OFFICIAL OFFICIAL - SENSITIVE *
RESTRICTED (high impact)	NHS Confidential	OFFICIAL - SENSITIVE *

* OFFICIAL - SENSITIVE is a sub-classification of the new central Government 'OFFICIAL' marking, where a more limited 'need to know' principle needs to be applied to information.