3Dimensions

Oct-18

Data Protection & Information Management Policy

Document Classification

PUBLIC

3Dimensions

Policy version control sheet

Document Status	**Current**
Policy Number	**27**
Version Number	**3**
Date of Policy	**Reviewed and updated 19.09.18**
Next review date	**September 2019**
Name of originator	**Shaun Davis (I.T Manager)**
Approved by	**Nita Ellul, Roz Simpson (Data Controller)**
Date of approval	**May 2018**
Target Audience	**Employees** **Referring authorities** **Parents and carers** **Regulatory bodies**
Links to other policies	*** Confidentiality & Privacy for YPs & Housemates policy** *** Case Recording & Access to Files.** *** Policy for Authorised Room searches** *** Internet Access & Online Safety policy** *** IT Access and Social Media for Staff** *** Password policy** *** Staff Mobile Phone policy** *** Safeguarding Children and Dealing with Allegations Policy**
Changes to previous version: Overhaul of policy to reflect GDPR, rework of policy for easier understanding and reading and amalgamation of two other policies – Encryption of confidential Data and Information Classification.	
Format Change: New Structure of Policy Outline, Policy Statement, Practical Guidance, Summary of Legislation and Learning Outcomes **Overhaul of Style structure to formatting 1. – 1.1 – 1.11** **Amended 19.09.18: Inclusion of the role of the Data Controller. Also see 3.3.7 In the case of a breach of data concerning children & YP's the Placing Authority's IT team should be contacted. In the case of a child or YP from Devon via a specific email and coordinated by the 3D data controller.**	

Distribution		
Intranet	Website (and in Online staff information)	Email to managers
✓	✓	✓

Document Classification

PUBLIC

3Dimensions

Table of Content

Definitions

Term	Definition
Must	This term is used to state a Mandatory action
Should	This term is used to state a Recommended action
Personal data	Any information including images relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Confidential Data	Racial/ethnic origin, political opinions, religious beliefs, trade union membership, and physical or mental health condition, details of their sexual life or their criminal record. Other examples include salary information, individuals' bank details, and passwords, of personally identifiable information including name, address, telephone number, and HR system data
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data processor	A person or other body, who processes personal data on behalf of 3 Dimensions Care.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1 Policy Outline

1.1 Introduction

1.1.1 3 Dimensions has a legal and professional duty to ensure the information we hold conforms to the principles of being:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

1.1.2 Information we are responsible for is processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. In addition, as a provider of Residential Children's Homes we also comply with the Children's Homes Regulations 2015 and other relevant regulations (see 1.2.2 below)

1.2 Purpose

1.2.1 The purpose of this policy is to enable all who process data for 3 Dimensions Care to understand their responsibilities concerning information.

1.2.2 To be fully aware of the requirements of the General Data Protection Regulation 2018, the Children's Act and Children's Homes Regulations 2015 or Care Quality Commission Outcome 12, and acts in accordance with data protection procedures.

Ensuring:

- Access to information is on a need to know basis, controlled and regularly reviewed
- The protection of all 3 Dimensions data and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of this data.
- We comply with all current and relevant UK and EU legislation.
- Provide a safe and secure environment for our employees and the people within our care
- The protection of 3 Dimensions from liability or damage through the misuse of its I.T facilities.
- A quick response to requests for information, feedback and updating as appropriate, initiating a cycle of continuous improvement.

1.3 Scope

1.3.1 This policy **must** be communicated to all applicable people and organisations who interact with information processed by or on behalf of 3 Dimensions.

1.3.2 All individuals and organisations who process personal information on 3 Dimensions behalf **must** act in line with this policy, and where applicable the Staff Contract of Employment, Staff Handbook or Consultancy Contract.

2 Policy Statement

2.1 Information Security Principles

The following governs the security and management of information

2.1.1 3 Dimensions Care and School is registered with the Information Commissioner's Office (ICO) and complies with the General Data Protection Regulation 2018 and is registered as a Data Controller and a Data Processor.

We have notified the Information Commissioner of:

- The personal data we process
- The categories of data subjects to which personal data relates
- The purposes of which the personal data will be processed

2.1.2 The requirements we have for processing personal data are recorded on the public register maintained by the ICO.

2.1.3 We renew our notification on an annual basis as the law requires. If there are any interim changes, these are notified to the ICO within 28 days.

2.1.4 We process information pertaining to our directors, employees, consultants, suppliers and the people in our care, for administrative, statutory, academic and health and safety reasons, to operate efficiently.

2.2 Collecting Personal Data

Lawfulness, fairness and transparency

2.2.1 We only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so we can **fulfil a contract** with the individual, or the individual has asked us to take specific steps before entering into a contract
- The data needs to be processed so we can comply with our legal obligation
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so we can perform a task in the **public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the company or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer where appropriate) has freely given clear **consent**

2.2.2 For special categories of personal data, we **must** meet one of the special category conditions for processing set out in the GDPR & Data Protection Act.

Limitation, minimisation and accuracy

2.2.3 We only process personal data for specified, explicit and legitimate reasons. We **must** explain these reasons to the individuals when we first collect their data.

2.2.4 If we want to use personal data for reasons other than those given when we first obtained it, we **must** inform the individuals concerned before we do so.

2.2.5 Individuals **must** only process personal data where it is necessary to do their jobs.

2.3 Children, Young People and Adults in Our Care

2.3.1 We are compliant with Children's Homes Regulations and Care Quality Commission standards in relation to the collection, storage and retention of records.

2.3.2 Further information on how we meet the requirements set out in the National Minimum Standard and Regulations for Children's Homes to ensure each child has a permanent, private and secure record of their history can be found in the following policies:

- Case Recording and Access to Files - Confidentiality and Privacy Policy

2.4 Document Classification

2.4.1 Different types of information require different security measures, making proper classification of information critical to effective security.

2.4.2 Information **must** be classified according to its level of sensitivity, confidentiality and risk of disclosure.

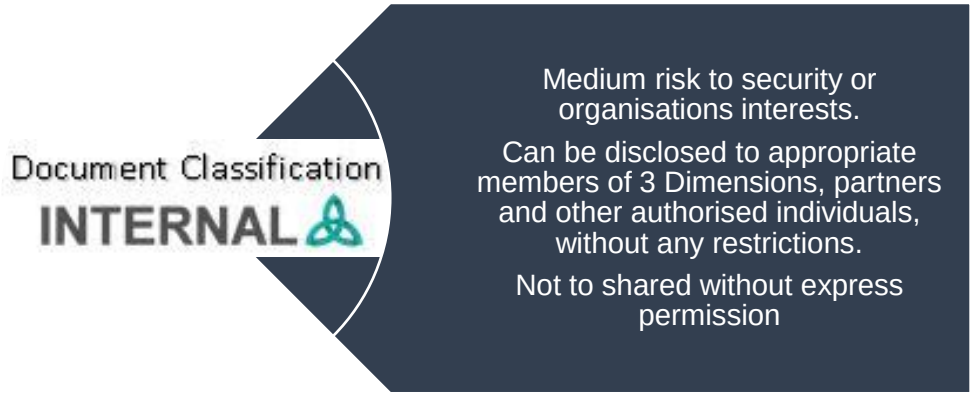
2.4.3 Individuals who process personal or confidential information are responsible for ensuring the classification of that information.

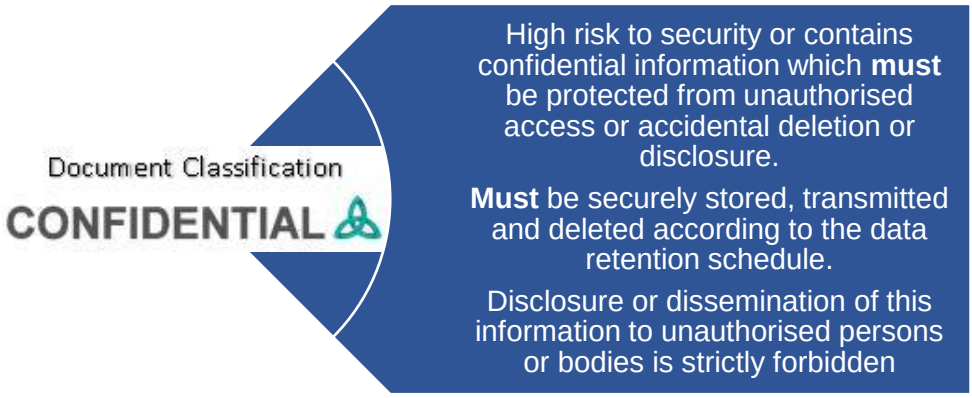
2.4.4 All individuals covered by the scope of this policy **must** respect information appropriately and in accordance with its classification level.

2.4.5 If confidential information is found, in an inappropriate place, you **must** report this to the I.T Manager as soon as possibly, who, depending on the circumstances, will inform the Data Controller and a Director..

2.4.6 You **must** assign one of the following three classifications to any information under your control:

2.5 Types of Classification Usage





2.6 Automatic File Classification

2.6.1 We use dynamic access control to identify personally identifiable information within documents to automatically assign access control to only authorised individuals regardless of location within our file servers.

2.6.2 Automatic File Classification is controlled by a set of pre-defined rules with the active directory linked to the different user groups.

2.7 Visual Classification Identification Marks

2.7.1 Visual classification identification marks can make documents easily identifiable as either Confidential, Internal or Public.

2.7.2 This prevents accidental disclosure of information due to documents being left in view if in hardcopy or on screens

2.7.3 For further information for adding a visual document classification identification to your documents, see the practical guidance section.

2.8 Data Protection and Awareness Training

2.8.1 Training is provided to all individuals on data protection awareness and sharing of information based on CWDC hand-outs, the care certificate workbook, information from the ICO and our own policies and guidance.

2.9 Disclosure of Information

2.9.1 We **do not** normally share personal data with anyone else, but may do so where:

- An issue with a person in our care or parent/carer which puts the safety of our employees or people in our care at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

2.9.2 Our suppliers or contractors need data to enable us to provide services to our employees or people in our care.

When doing this, we:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with Data Protection Law
- Establish a data sharing agreement with the supplier or contractor, either in a contract or as a standalone agreement

2.9.3 To ensure the fair and lawful processing of any personal data we share we **must**:

- Only share data when the supplier or contractor needs to carry out their service, and provide them with information necessary to keep them safe while working with us

2.9.4 We also share personal data with law enforcement and government bodies where we are legally required to do so, including for the following:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- Relating to legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Statistical purposes, if personal data is sufficiently anonymised or consent has been provided

2.9.5 We may also share personal data with emergency services and local authorities to help them to respond to an emergency that can affect any of our employees or people in our care.

2.9.6 Where we transfer personal data to a country or territory outside the European Economic Area, we **must** do so in accordance with data protection law.

2.10 Prevention of Casual or Accidental Disclosure

2.10.1 Any confidential information, including personal data of people in our care or employment, **must** not be disclosed either orally or in writing accidentally to any unauthorised third party.

2.10.2 Often confidentially is broken not through normal day-to-day work routines but through accidental disclosure

We ensure accidental disclosure does not take place by:

- Not leaving confidential paperwork in view on desks
- Not allowing unauthorised individuals to view computer screens.
- Locking PC and laptop screens when unattended.
- Keeping confidential paperwork securely stored, and destroying it in a confidential manner using an approved shredder
- Keeping conversations regarding confidential topics private and away from hearing distance of unauthorised individuals

2.11 When We Do Disclose Information

2.11.1 Personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent
- Where the disclosure is in the legitimate interests of the organisation
- Employees require the information to enable them to legitimately perform their jobs
- Where the organisation is legally obliged to disclose the data i.e. Safeguarding
- Where disclosure of data is required for the performance of a contract

2.11.2 If consent for disclosure has not been given and the reason is not one detailed above, you **must** decline to comment.

2.11.3 Even confirming if an individual is a member 3 Dimensions Care and School may constitute an unauthorised disclosure.

2.11.4 The enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure.

2.12 Exceptions to Standard Disclosure Procedures

2.12.1 Where a disclosure is requested in an emergency, you **must** make a careful decision, considering the nature of the information being requested and the likely impact on the data subject of providing or not providing it.

2.12.2 The protection, safety and welfare of individuals in our care takes precedence over issues of confidentiality.

2.12.3 If you are concerned an individual in our care has or may have been abused, you **must** report this immediately to the Company's Responsible Individual and designated Safeguarding Officer.

2.12.4 You should refer to 3 Dimensions' Safeguarding and Dealing with Allegations Policy for further detailed guidance.

2.12.5 If in doubt, you **must** seek advice from your Manager.

2.12.6 Further information and guidance can be found in the Data Protection section of the Staff Handbook.

2.13 Dealing with Information Requests

2.13.1 Where non-routine requests are made, or where you are unsure you **must** seek the advice of your Manager.

2.13.2 Managers may decide to refer a request for a definitive decision to the Data Controller or a Company Director.

2.13.3 You **must** be aware, those seeking information may use deception to obtain information.

2.13.4 You **must** verify the identity of those seeking information, for example by obtaining and verifying the telephone number and returning the call or by reviewing identification documents if an application is made in person.

2.13.5 All applications for data **must** be made in writing. Only in extreme circumstances can any non-routine application be accepted verbally

2.13.6 Request by public bodies, including the police, **must** meet the requirements for lawful processing.

2.14 Subject Access Requests

2.14.1 Individuals have a right to make a 'subject access request' to gain access to personal information we hold about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

2.14.2 Subject Access Requests **must** be submitted in writing, either by letter or email to the Responsible Individual. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

2.14.3 If you receive a Subject Access Request, they **must** immediately forward it to the Responsible Individual, The It Manager and the Data Controller.

2.15 Children Within Our Care and Subject Access Requests

2.15.1 Personal data about a child belongs to that child. If a young individual in our care or who has been in our care makes a Subject Access Request, more information can be found for them in the:

- Access to Care Records and Consent Policy

2.15.2 This explains how to access any social care records that we hold about them, together with the process to follow if they wish to see their records and are no longer in our care.

2.16 Parent or Carer Access Requests

2.16.1 For a parent or carer to make a Subject Access Request with respect to their child, the child **must** either be unable to understand their rights and the implications of a Subject Access Request, or have given their consent.

2.16.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, Subject Access Request from parents or carers may be granted without the express permission of the child.

2.16.3 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers may not be granted without the express permission of the pupil.

2.16.4 Whether a child is under the age of 12 or not, the capacity of the child, the ability to understand their rights is always judged on a case-by-case basis.

2.17 Responding to Subject Access Requests

2.17.1 When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Must respond without delay, within 1 month of receipt of the request
- Must provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

2.17.2 We **do not** disclose information if it:

- Might cause serious harm to the physical or mental health of the data subject or another individual
- Would reveal the data subject is at risk of abuse
- Where the disclosure of information would not be in the data subject's best interests
- Is given to a court in proceedings concerning the data subject

2.17.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

2.17.4 A request is deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

2.17.5 When we refuse a request, we tell the individual why, and tell them they have the right to complain to the ICO.

2.18 Other Data Protection Rights of The Individual

2.18.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data, how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

2.18.2 Individuals should submit any request to exercise these rights to the Responsible Individual. If you receive such a request, you **must** immediately forward it to the Responsible Individual.

2.19 Data Security and Storage of Records

2.19.1 We protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

By making sure:

- All offices where processing of personal data occurs **must** be locked when not occupied.
- Paper records and portable electronic devices, containing personal data **must** be kept under lock and key when not in use, where access is restricted to Senior Managers and other authorised personnel.

- Paperwork containing confidential personal data **must not** be left on desks, pinned to notice boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, it **must** be signed in and out from the main office
- Passwords **must** be at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices (see the password policy).
- We have taken precautions to ensure the data security of our data systems and backups.
- Individuals **must** not have access to information to which they do not have a legitimate right.
- The level of access for each user is defined and controlled in the domain group policy manager.

2.20 Removable Storage

2.20.1 We restrict the use of removable media where possible. If removable media is granted:

- We will provide you with an encrypted USB drive.
- Only removable storage devices supplied by 3 Dimensions may be used.
- USB drives are not to be taken off site

2.20.2 If you need access to work files at home please talk to your Manager who can request for a secure laptop for you to connect to work from home

2.21 Sending Confidential or Personal Information

2.21.1 Care **must** be used before deciding to transmit personal or confidential data by post or email. If emails are sent containing confidential information, then encryption **must** be used. Please read practical guidance below for information on using egress to encrypt emails

2.21.2 When sending confidential information via postal services it is required the recipients address is checked before the information is sent.

2.21.3 Before sending, the envelope **must** be clearly addressed, sent using the recorded and signed for postal service with a clear return address.

2.22 Encryption of Data

What is encryption?

2.22.1 Encryption is a way of making information so it cannot be read without the appropriate key to decode it. It is a way of rendering files, volumes or hard disks extremely secure.

When must encryption be used?

2.22.2 Encryption **must** be used to secure data when in transit or accessed outside

2.22.3 3 Dimensions systems, for instance on an offsite workstation, or on devices which are easy to steal or lose (such as laptops, tablets etc.).

What must be encrypted?

2.22.4 Not all of 3 Dimensions data is so confidential it needs to be encrypted in transit, however all data at rest is encrypted when stored upon our file servers, workstations and laptops.

2.22.5 Data which **must** be encrypted during electronic transit is all sensitive, personal or confidential data including the following:

- Financial information relating to individuals in our employment or care
- Any type of account details
- Personal, identifiable information
- Legal data
- Confidential Business & Intellectual Property

2.22.6 It is your responsibility to assess the data requirements of the information you are using and take responsibility for the measures you use to protect them.

2.22.7 Generally, any classified document other than **PUBLIC** may need to be encrypted

2.23 The Use of Company Computers for Personal Use

2.23.1 The company computers are for business use, excessive personal use is not allowed.

2.23.2 You **must** be aware all information on computers belongs to 3 Dimensions.

2.23.3 We therefore monitor the use of computers and network resources regularly, including all internet usage, file access, system access and modification.

2.23.4 Internet access for personal use is permitted if it is during break times and not excessive

2.23.5 **DO NOT USE** workstations for private matters such as personal email, online banking, social media or other such tasks as your information will be logged

2.23.6 Further information and guidance can be found in the Use of Computer and Telecommunication Services section of the Staff Handbook and in other related policies.

2.24 Retention of Personal Data

2.24.1 We do not keep personal data for longer than required by law. Some data is kept for longer periods than others.

2.24.2 We manage the retention of personal data through a regularly reviewed documentation data controller spreadsheet which defines the retention schedule for the different types of personal data we process

2.24.3 In general, electronic staff records containing information about individual members of staff and other specified records are kept in accordance with The Children's Homes (England) Regulations 2015 as per regulation 37 and as set out in schedule 4 for at least 15 years after the last entry. Information would typically include name and address, position held, leaving salary etc.

2.24.4 Other information relating to individual members of staff is kept by Human Resources for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc., is retained for the statutory time period (between 3 and 6 years).

2.24.5 Children Case Records with direct relevance to Children and Young people and/or Vulnerable Adults are kept for 75 years from the date of birth of the child/adult or if the child dies in our care before the age of 18, for 15 years from the date of his or her date of death.

2.24.6 Information relating to unsuccessful applicants relating to recruitment to a post is generally destroyed after one month, apart from the recruitment form which is held for one year before being securely destroyed.

2.25 Disposal of Personal Data

2.25.1 Care **must** be taken with the disposal of personal data. Personal data **must** be disposed of in a way that protects the rights and privacy of data subjects and is irretrievably destroyed.

2.25.2 You should be aware the same standards **must** be applied to informal paperwork or lists held by individual members of staff containing personal data.

2.25.3 Personal data **must** be destroyed by secure methods such as shredding or secure electronic deletion. Hard drives of redundant PCs or laptop computers are wiped clean beyond the possibility of recovery.

2.25.4 Where personal data is to be deleted, the files containing the data **must** be deleted and any recycle bin emptied.

2.25.5 Formal records both hardcopy and electronic may only be destroyed with the appropriate authorisation.

2.25.6 All destruction of formal records **must** be recorded in the retention and destruction of data spreadsheet by an authorised person

2.25.7 Hardcopies which are no longer current but which the company is required to keep by law for long periods are archived and stored in a secure location, fire and flood proof building until they are electronically archived, by an authorised member of staff.

2.25.8 When this takes place, the document is to be saved in PDF format with a digital certificate attached certifying its accuracy and integrity

2.26 Enforcement

2.26.1 Regular assessments are carried out to see how well our policy and processes are working.

2.26.2 This is not to apply individual penalties associated with failing to comply with policy. Security comes first, and this can only happen if:

- You are aware and happy with the procedure and systems in place

- You feel safe to report security breaches or mismanagement without worry of penalty

2.26.3 Intentional disregard of this policy unrelated to difficultly to understand or implement procedures may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

3 Data Breach Incident Handling

3.1.1 A loss or breach of data may result in the possible loss of confidentiality, integrity and availability of personal or other confidential data

This may result in

- The loss of business
- Financial penalties
- Criminal or Civil Action against 3 Dimensions

3.1.2 Therefore, it is essential any breaches of this policy **must** be reported immediately to your Manager, IT Manager or one of the Directors

3.1.3 If necessary you can use 3 Dimensions Whistle Blowing Policy or by contacting ICO directly.

3.2 Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

3.2.1 On finding or causing a breach, or potential breach, you **must IMMEDIATELY** notify the I.T Manager, The Data Controller, and your Manager

3.2.2 The I.T Manager investigates the report,and determines whether a breach has occurred. To decide this, the I.T Manager and the Data Controller, considers whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

3.2.3 The I.T Manager and Data Controller **must** alert the relevant members of management, including the Data Controller and Directors

3.2.4 Management **must** make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

3.2.5 The I.T Manager, Data Controller and Directors assess the potential consequences, based on how serious they are, and how likely they are to happen.

3.2.6 The I.T Manager, Data Controller, and Directors will work out whether the breach must be reported to the ICO. This is judged on a case-by-case basis.

3.2.7 To decide, we consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage including via the following:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

3.2.8 If it's likely there is a risk to people's rights and freedoms, we **must** notify the ICO.

3.3 Decision Outcome

3.3.1 We **must** document the decision (either way), in case it is challenged by the ICO or an individual affected by the breach.

3.3.2 Where the ICO should be notified, the I.T Manager, Data Controller or Director **must** do this via the 'Report a Breach' page of the ICO website within 72 hours. As required we set out a description of the personal data breach.

including, where possible:

- The categories and approximate number of individuals concerned
- The approximate number of personal data records concerned
- The name and contact details of the person dealing with the breach
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

3.3.3 If all the above details are not yet known, the I.T Manager, Data Controller or Directors. **must** report as much as they can within 72 hours.

3.3.4 The report explains there is a delay, the reasons why, and when we expect to have further information.

3.3.5 We **must** submit the remaining information as soon as possible

3.3.6 The I.T Manager, Data Controller and Directors also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, we then promptly inform, in writing, all individuals whose personal data has been breached.

3.3.7 We may notify any relevant third parties who can help mitigate the loss to individuals. In the case of a breach of data concerning children & YP's the Placing Authority's IT team should be contacted. In the case of a child or YP from Devon: **Devon County Council requires companies and other persons to have appropriate standards in place to protect its data. Security incidents must be reported to: KeepDevonsDataSafe@devon.gov.uk These include, but are not limited to, unauthorized access, denial of service, loss or theft of information and data corruption.**

3.3.8 The person, usually the Data Controller in conjunction with the I.T Manager, dealing with the breach **must** document each breach, irrespective of whether it is reported to the ICO. For each breach, this record includes the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

3.3.9 Records of all breaches **must** be stored in a secure access restricted folder upon our file servers.

3.4 Summary of Relevant Legislation

3.4.1 This policy was created to adhere to legislation, recommendations and guidance from the Acts and Regulation below. If you wish to view them in their entirety please click on a link below

3.4.2 The Computer Misuse Act 1990

3.4.3 General Data Protection Regulation 2018

3.4.4 The Freedom of Information Act 2000

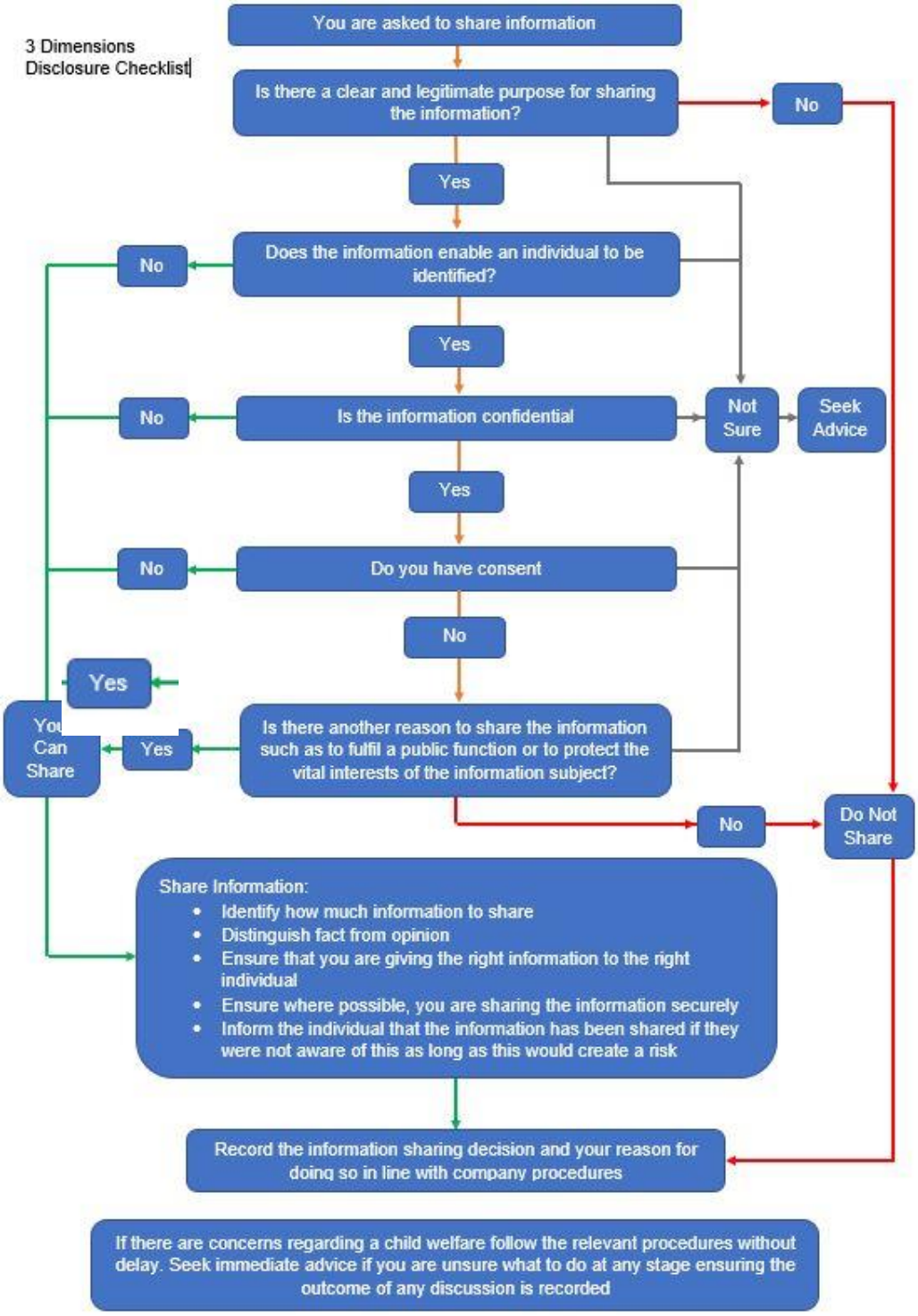
3.4.5 Regulation of Investigatory Powers Act 2000

4 Practical Guidance

4.1 How to Decide to Disclose Information

4.1.1 Before disclosing personal information run through the checklist below to decide if the discloser is necessary

3 Dimensions
Disclosure Checklist



4.2 Request for Information Over the Telephone

4.2.1 In general, disclosures to external bodies/companies/agencies/individuals **MUST NOT** be made over the telephone.

4.2.2 Follow the steps below when asked to disclose information over the telephone which is not part of your routine business duties

Step 1

- Ask for the request in writing where possible. Only in exceptional circumstances should confidential and personal identifiable information be disclosed
- Ask what information is requested and the purpose of the request
- Make sure you can authenticate the identity of the caller by taking a contact number and call them back

Step 2

- Before calling them back seek advice from your Manager if you are unsure.
- Always be cautious when talking to unknow people, make sure not to answer leading questions or to be pressured into giving information
- Separate fact from opinion when it comes to the emergency of the request
- Avoid confirming any details of the data subject - even their presence in the organisation.

Step 3

- If disclosure of information is absolutely necessary take care to give the minimum amount of information required to fulfil the request

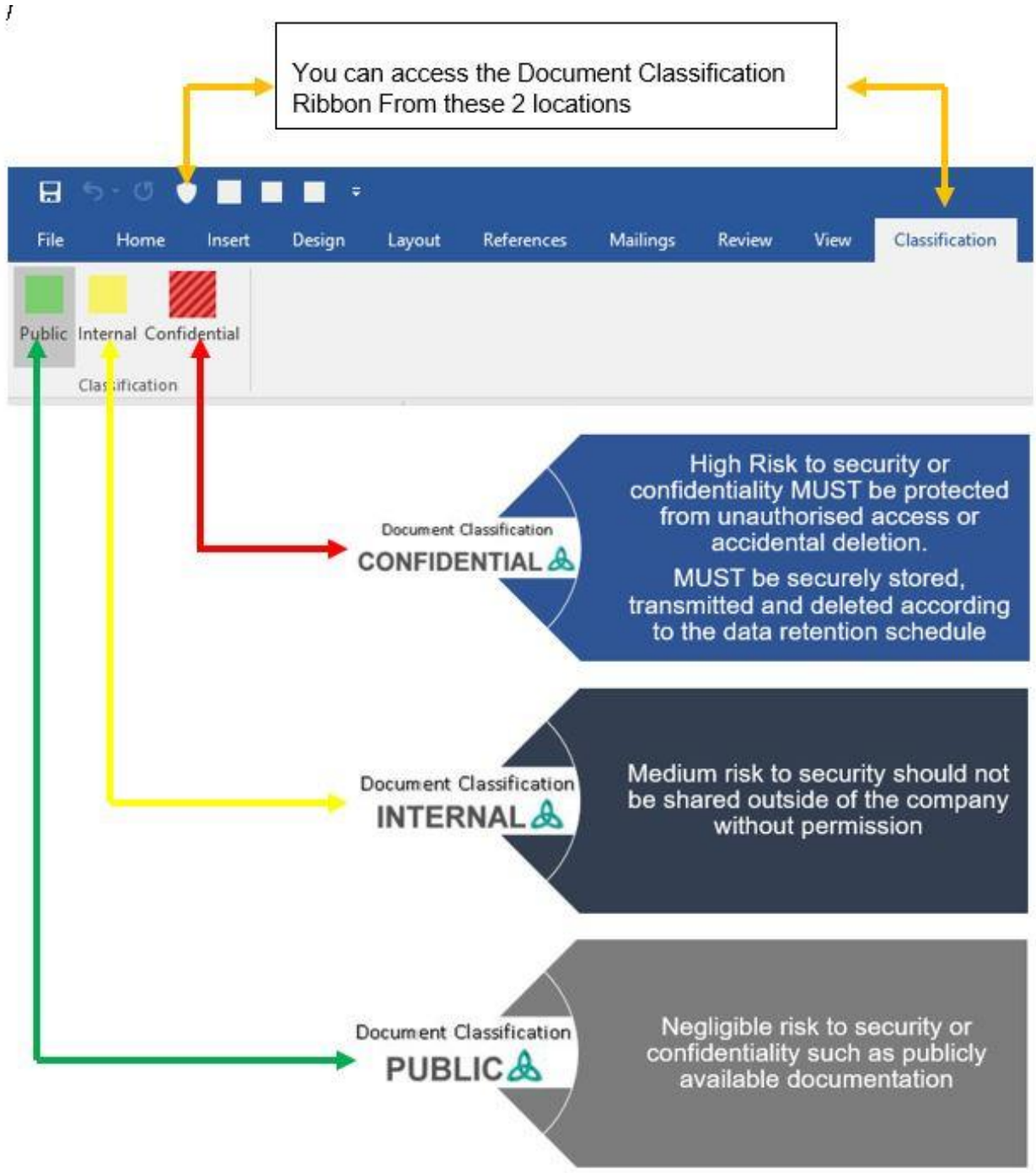
Step 4

- As soon as the conversation is over document what was discussed, any advice you saught before returning the call and the outcome of the request.

4.3 Using the Document Classification Ribbon

4.3.1 If Authorised the I.T Department will install a document classification ribbon within word and Excel to enable you to visually classify documents at the point of creation

See below:



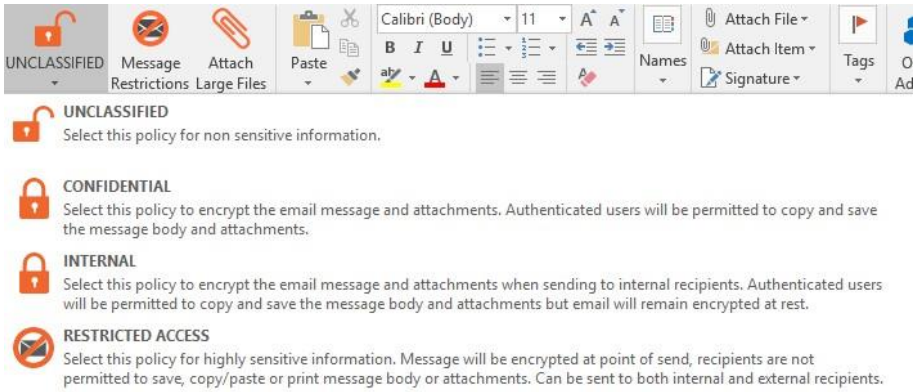
4.4 Using the Egress in Microsoft Outlook

4.4.1 The Egress Switch Outlook add-in provides transparent secure email creation from within Outlook. When the Switch Outlook Add-in is installed, extra buttons become available in the ribbon:

Sending a secure email

4.4.2 Open a new message in Outlook, completing the To, Cc and Subject fields and composing your message as normal.

4.4.3 To send the email securely, click on the Switch dropdown menu and choose your desired encryption type. The options available here are dictated by your business account's policy and so some options may not be available.



1. Press **Message Restrictions** to configure time restrictions for the secure email. These restrictions are optional and can be changed at any point, even after the email has been sent.

2. Press **Send** as usual once your message is complete.

5 Policy Outcomes

5.1 What are the Policy Outcomes?

5.1.1 Below is a list of the outcomes from this policy. Policy outcomes are key information which you **must** always adhere to.

5.1.2 This list is used as a quick reference guide but **must** not replace reading the policy in its entirety.

5.1.3 Information not in this list but in the policy statement is **NOT** any less important

Key Information

- If you are unsure regarding this policy you **must** seek advice
- Unauthorised disclosure, failure to report breaches or disregard for this policy may be regarded as a disciplinary matter.
- Information **must** be classified appropriately
- You **must** use secure systems when storing personal data or sending it by post or email
- You **must** seek the advice of your Manager or Director before any disclosure.
- Non-routine requests **must** not be accepted over the phone unless in exceptional circumstances
- Where a disclosure is requested in an emergency, you **must** decide to disclose considering the impact of disclosing may have on the data subject
- You **must** not disclose any personally identifiable information before you can confirm the identity and legitimacy of the request.
- Everyone has the right to request in writing, the information we hold regarding themselves when we are the data originators.
- Safeguarding, prevention of crime or harm and national security override issues of confidentiality.
- You **must** not intently access information to which you do not have a legitimate access right.
- Personal information **must** not be kept for longer than it is legally needed.
- Data of previous employees or placements **must** be archived adequately
- You **must** not use your own devices to access our work network, work on company material or hold information without explicit written consent
- IT equipment we own is for business use only.
- We monitor and audit the use of our computer and network resources
- You **must** ensure casual or accidental disclosure does not take place
- Data **must** be disposed of in a way that protects the rights of data subjects
- Any breaches of this policy **must** be reported immediately to your Manager
- You are also able to use 3 Dimensions Whistle Blowing Policy or by contacting ICO directly.