Information Management Standards

Organisation	London Legacy Development Corporation
Date	2013-10-14
Purpose of issue	For information
Title	Information Management Standards
Description	Describes a set of standards for version control, the control of documents, the transfer of data and the management of email
Author	Danny Budzak
Location	O:\Departments\Finance & Corporate Services\IT&IS\Standards
Contributors	Jim Wood, Rachael Clauson
Distribution	All staff
Status	Version 1.0, approved by EMT
Protective marking	Not Protectively Marked

Version Control

Version	Date	Amendments	Author
v1.0	2013-10-14	Summary of Information Management Standards draft	Danny Budzak

Introduction

This is a summary of the Information Management Standards document that can be found on the intranet (http://intranet.londonlegacy.co.uk/information-technology/managing-your-records-and-information.aspx)

The following standards must be followed by all LLDC staff to ensure that data and information is effectively managed and controlled.

- Document control template
- Version control template
- Data transfer
- Email management

1. Document Control Template

The document control template is used to describe key elements of the document. An example of the use of document and version control are on the front page of this document.

Organisation	*EITHER London Legacy Development Corporation* *OR* *E20 Stadium LLP*
Date	*The date created or published*
Purpose of issue	*Why the document has been created: approval, comment, information*
Title	*The person who has created the document*
Description	*Brief description of one sentence.*
Author	*The person who has created the document*
Location	*The location where the file is filed – for example:* *O:\Departments\Finance & Corporate Services\IT&IS\Standards*
Contributors	*Any one who has contributed to the document*
Distribution	*List of everyone who has received the document*
Status	*Draft OR Published*
Protective marking	*Protectively marked OR Not Protectively Marked – for guidance see the intranet (http://intranet.londonlegacy.co.uk/protective-marking.aspx)*

2. Version Control

The purpose of version control is to ensure that the most recent document is being used, and everyone is referring to the same content.

Version control also helps to describe what stage a piece of information is at and how it has changed over time. This includes whether it is a draft or published version.

Where several people are working on the same document, care must be taken in controlling the versioning, and it may be more effective to have one person with that responsibility.

The following standard should be followed:

v0.1 Document created. This is the first draft.

v0.2 Changes to the document. This could be as the document progresses or based on feedback and consultation.

v0.3, v0.4, v0.5.....onwards. These are all drafts.

v1.0 This is a document which has been issued to business users or published to external stakeholders. It is the first published version.

v1.1 This is minor amendments to the document. This is still a published or issued version.

v2.0 This is a substantial change to a document. For example, a policy document which has been thoroughly reviewed and changed following consultation with stakeholders

If the document has a single author who is making daily changes, over a period of time, there is no need to change the version number each time a minor amendment is made.

When the first published version is released, all of the version history can be replaced with a new table:

Version	Date	Description	Author
v1.0	2013-07-23	First published version	

Please note: Use v0.xx for all versions until final sign off. After sign off, v1.0 should be used.

Date: The date format of yyyy/mm/dd is the international standard and should be used in the version control table.

Footer

The footer should include the document filename which will include the version number.

Retention of Previous Versions

The retention or disposal of a series of versions will be determined by business needs.

There is no need to retain earlier versions of most documents. In practice retaining versions which have been superseded simply creates an information overload which can be avoided.

3 Data Transfer Standards

Data transferred between the Legacy Corporation and any other organisation or person must be done in a secure way to ensure compliance with the law, including Freedom of Information and Data Protection. It is important that data is not lost and the reputation of the Legacy Corporation is protected.

Acceptable

The following are all acceptable ways to transfer data. For more information including usage see the Information Management Standards document on the intranet.

Secure FTP is a way of transferring large files from one computer to another over the internet.
To get an account set up contact the Civica helpdesk (lldcsupport@civica.co.uk or x4357).
The ftp address is https://ftp.civicahosting.co.uk

Encrypted USB keys. These are available from IT&IS. The receipt and return of the encrypted USB keys must be signed for.

Encrypted Portable Hard Drives. These are available from IT&IS. The receipt and return of the encrypted portable hard drives must to be signed for.

Email. The maximum size of a file which can be sent by email is 10MB.

Ensure that you check recipients names as the auto-complete feature of Outlook can mean the wrong name is chosen.

Take care when emailing to the public as sharing personal information such as email addresses without consent is a breach of the Data Protection Act.

Not Acceptable

The following are not acceptable ways of transferring information outside the Legacy Corporation.

Email to Personal Email Accounts. Legacy Corporation data and information should not be sent by staff to their own personal email accounts. This has Freedom of Information and Data Protection implications. The Legacy Corporation provides a system whereby staff can have remote access to the O drive and email via Citrix. This can be used on any occasion where work is being done outside the office.

Unencrypted Data Sticks. There is a reputational risk to the Corporation if an unencrypted USB key is used to transfer documents. There is also a security risk if sensitive material is moved in this way.

CDs. These are not a secure medium and cannot be encrypted. Even if the content is not confidential or sensitive, the lack of security could have reputational impact.

File Formats (for external transfer)

PDFs. The recommended file format for document transfer is PDF. This should be used for any document which is being sent to an external organisation which does not require tracked changes. While PDFs can be altered, this is not as easy to do as altering a word document.

Spreadsheets. Where spreadsheets are being transferred, a check should be made to ensure there are no comments which are only intended for internal use or additional worksheets (tabs) that should not be shared.

A document control template should be created as part of one of the worksheets to enable the provenance to be understood.

4 Email Management

Email is a key business tool with multiple uses. It supports communication, workflow and decision making. Emails can be business records which need to be retained for specific periods of time. These rules describe ways in which email can be managed more effectively.

Compliance

The Legacy Corporation is subject to a framework of legislation including Freedom of Information (FOI) and Data Protection. This means that any email could be subject to an FOI request, or a Subject Access Request. Any individual can ask the Legacy Corporation for details of all the data held about them – including that held in emails.

Emails could be requested by a court of law, a tribunal or an internal review.

If personal email accounts are used for Legacy Corporation business (in contravention of this policy), then the contents will become subject to FOI and Data Protection.

Risks

If email accounts are not managed properly, then the following risks increase:

- Personal data being retained within emails which should have been deleted to ensure compliance with the Data Protection Act
- Having to work with large volumes of emails in response to an FOI request
- Increasing costs of storage, back up and restoration of systems
- Making it harder to find content

Mailbox Clean Up. This Outlook function enables all the emails to be sorted regardless of whether they are in the Inbox, Sent Items or individual folders. They can then be deleted as needed.

Managing the Mailbox. Emails can be sorted, filed and searched according to various criteria.

Deleting Mail. When emails are deleted, they are moved to the Deleted Items folder. This then needs to be emptied to free up mailbox space.

Attachments. There is no need to send attachments internally. It is much more effective to send a link to a file on the O drive. Attachments can be easily removed from emails; this is a useful way to reduce the size of mailboxes, and retain the original email.

Email Archive. All email is archived in an area called the Symantec.cloud. Even when email has been deleted from an individual mail box, there is still a copy in the Symantec.cloud. The archive can be searched using a range of criteria.

Tips on Managing Email Effectively

- Remove large attachments – store them on the O drive
- Set aside 10 minutes a week to manage emails
- Collate emails which can be deleted in bulk – for example, meeting acceptances
- Try to reduce the number of people who are cc'ed into emails
- Read and delete where possible