From: [redacted]
Sent: 28 February 2016 09:54
To: FOI
Subject: Freedom of Information request: Boundary Commission for England (Advisory NDPB)

Dear Sir or Madam

I am writing under the Freedom of Information Act 2000 to request details of breaches of the Data Protection Act within in your organisation; specifically I am asking for:

1a. Approximately how many members of staff do you have?
1b. Approximately how many contractors have routine access to your information?

2a. Do you have an information security incident/event reporting policy/guidance/management document(s) that includes categorisation/classification of such incidents?
2b. Can you provide me with a copy of the latest version of these document(s)? (This can be an email attachment or a link to the document on your publicly facing web site)

3a. Do you know how many data protection incidents your organisation has had since April 2011? (Incidents reported to the Information Commissioners Office (ICO) as a Data Protection Act (DPA) breach)
Answer: Yes, No, Only since (date):
3b. How many breaches occurred for each Financial Year the figures are available for?
Answer FY11-12: FY12-13: FY13-14: FY14-15:

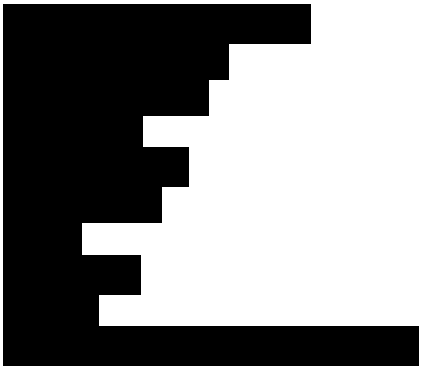
4a. Do you know how many other information security incidents your organisation has had since April 2011? (A breach resulting in the loss of organisational information other than an incident reported to the ICO, eg compromise of sensitive contracts or encryption by malware.)
Answer: Yes, No, Only since (date):
4b. How many incidents occurred for each Financial Year the figures are available for?
Answer FY11-12: FY12-13: FY13-14: FY14-15:

5a. Do you know how many information security events/anomaly your organisation has had since April 2011? (Events where information loss did not occur but resources were assigned to investigate or recover, eg nuisance malware or locating misfiled documents.)
Answer: Yes, No, Only since (date):
5b. How many events occurred for each Financial Year the figures are available for?
Answer FY11-12: FY12-13: FY13-14: FY14-15:

6a. Do you know how many information security near misses your organisation has had since April 2011? (Problems reported to the information security teams that indicate a possible technical, administrative or procedural issue.)
Answer: Yes, No, Only since (date):
6b. How many near-misses occurred for each Financial Year the figures are available for?
Answer FY11-12: FY12-13: FY13-14: FY14-15:

If the specific answers to 4, 5 and 6 are not readily available, I am content for these questions to be modified/replaced with similar questions that are derived from your organisations categorisation/classification system within the documents requested in question 2. I would need to first make an FoI request for question 2 in order to frame suitable questions 4, 5 and 6, then make a second request. Similarly calendar year can replace financial year. Please state in the reply if this option has been implemented. My preferred format to receive this information is electronically, but if that is not possible I will be willing to accept hard copy. I would be grateful if you could include my reference

Ref: 805051



This concludes the Freedom of Information request.

As a general enquiry
Would someone from the information security structure (CISO or information security manager) consider being approached to partake in academic research in to security incident and event reporting? This academic research would ensure respect any wish for anonymity and anonymising of data supplied. The format of any proposed research would be less than a dozen questions, provided in advance, and followed by an interview. If after considering the questions your organisation is content, we will arrange the interview that is not intended to exceed 30 minutes. This is likely to be early summer 2016.

If someone is willing to participate in this research, would you provide me with a name and contact email by email outside of the FoI request.

Regards
[redacted]

From: Cleverly, Karen
Sent: 02 March 2016 10:34
To: [redacted]
Subject: Freedom of Information Request - your ref 805051

Dear [redacted],

FOI Ref: 01/16

You requested:

"details of breaches of the Data Protection Act within in your organisation; specifically you asked:

1a. Approximately how many members of staff do you have?

1b. Approximately how many contractors have routine access to your information?

2a. Do you have an information security incident/event reporting policy/guidance/management document(s) that includes categorisation/classification of such incidents?

2b. Can you provide me with a copy of the latest version of these document(s)? (This can be an email attachment or a link to the document on your publicly facing web site)

3a. Do you know how many data protection incidents your organisation has had since April 2011? (Incidents reported to the Information Commissioners Office (ICO) as a Data Protection Act (DPA) breach)

Answer: Yes, No, Only since (date):

3b. How many breaches occurred for each Financial Year the figures are available for?

Answer FY11-12: FY12-13: FY13-14: FY14-15:

4a. Do you know how many other information security incidents your organisation has had since April 2011? (A breach resulting in the loss of organisational information other than an incident reported to the ICO, eg compromise of sensitive contracts or encryption by malware.)

Answer: Yes, No, Only since (date):

4b. How many incidents occurred for each Financial Year the figures are available for?

Answer FY11-12: FY12-13: FY13-14: FY14-15:

5a. Do you know how many information security events/anomaly your organisation has had since April 2011? (Events where information loss did not occur but resources were assigned to investigate or recover, eg nuisance malware or locating misfiled documents.)

Answer: Yes, No, Only since (date):

5b. How many events occurred for each Financial Year the figures are available for?

Answer FY11-12: FY12-13: FY13-14: FY14-15:

6a. Do you know how many information security near misses your organisation has had since April 2011? (Problems reported to the information security teams that indicate a possible technical, administrative or procedural issue.)

Answer: Yes, No, Only since (date):

6b. How many near-misses occurred for each Financial Year the figures are available for?

Answer FY11-12: FY12-13: FY13-14: FY14-15:"

The Commission aims to respond promptly and within the statutory deadline of 20 working days set by the Freedom of Information Act 2000. Please expect a response by **28 March 2016**.

In some cases a fee may be payable and if that is the case I will let you know. A fees notice will be issued to you, and you will be required to pay before I will proceed to deal with your request.

If you have any queries or concerns please do not hesitate to contact me on the details provided below. Please remember to quote the reference number above in any future communications.

Regards,

Karen Cleverly
Business Support Officer
Local Government Boundary Commission for England
14th Floor, Millbank Tower
Millbank
LONDON
SW1P 4QP

Tel: 0330 500 1260
www.lgbce.org.uk

@lgbce

It would help us if you would take a few minutes to answer a few questions about your experience of how we dealt with you.

How are we doing? - Click on this link to give us your views

From: Cleverly, Karen
Sent: 22 March 2016 09:55
To: [redacted]
Subject: Freedom of Information Request - your ref 805051
Attachments: ICT Acceptable Use Policy - FINAL 1 Dec 2010.doc; Information Management & Security FINAL 2016.03.09.docx; Personal Data Policy - FINAL - 1 Dec 2010.doc; [redacted] Response-2016-03-22.docx

Dear [redacted],

FOI Ref: 01/16

Please find attached our response to your request, along with relevant documents.

We would prefer not to take part in the research project.

Regards

Karen Cleverly
Business Support Officer
Local Government Boundary Commission for England
14th Floor, Millbank Tower
Millbank
LONDON
SW1P 4QP

Tel: 0330 500 1260
www.lgbce.org.uk

@lgbce

It would help us if you would take a few minutes to answer a few questions about your experience of how we dealt with you.

How are we doing? - Click on this link to give us your views

The Local Government Boundary Commission for England

[redacted]

BY EMAIL

22 March 2016

Dear [redacted],

Our Ref: FOI 01/16 Your Ref: 805051

Thank you for your email of 28 February 2016 requesting information under the Freedom of Information Act 2000.

The Commission does hold information relevant to your request. Please find below a list of our responses to the information you have requested:

1a. Approximately how many members of staff do you have?
We have 22 members of staff.

1b. Approximately how many contractors have routine access to your information?
Four.

2a. Do you have an information security incident/event reporting policy/ guidance/management document(s) that includes categorisation/classification of such incidents?
Yes.

2b. Can you provide me with a copy of the latest version of these document(s)?
I have attached copies of the following policies:

- *ICT Acceptable Use Policy*
- *Information & Security Policy*

- *Personal Data Policy*

Please note that these policies are in the process of being reviewed and updated.

3a. Do you know how many data protection incidents your organisation has had since April 2011? (Incidents reported to the Information Commissioners Office (ICO) as a Data Protection Act (DPA) breach)
Yes.

3b. How many breaches occurred for each Financial Year the figures are available for?
FY11-12: *None* FY12-13: *None* FY13-14: *None* FY14-15: *None*.

4a. Do you know how many other information security incidents your organisation has had since April 2011? (A breach resulting in the loss of organisational information other than an incident reported to the ICO, eg compromise of sensitive contracts or encryption by malware.)
Yes.

4b. How many incidents occurred for each Financial Year the figures are available for?
FY11-12: *None* FY12-13: *None* FY13-14: *One* FY14-15: *None*.

5a. Do you know how many information security events/anomaly your organisation has had since April 2011? (Events where information loss did not occur but resources were assigned to investigate or recover, eg nuisance malware or locating misfiled documents.)
Yes.

5b. How many incidents occurred for each Financial Year the figures are available for?
FY11-12: *None* FY12-13: *None* FY13-14: *One* FY14-15: *None*.

6a. Do you know how many information security near misses your organisation has had since April 2011? (Problems reported to the information security teams that indicate a possible technical, administrative or procedural issue.)
Yes

6b. How many near-misses occurred for each Financial Year the figures are available for?

FY11-12: *None* FY12-13: *None* FY13-14: *None* FY14-15: *None*.

If you have any further queries, please do not hesitate to contact me, quoting the reference number above in any correspondence.

If you wish to request a review of our decision, you should write to:

Lynn Ingram
Director of Finance
Local Boundary Commission for England
14th Floor, Millbank Tower
Millbank
London
SW1P 4QP

If you are not content with the outcome of your complaint or review, you may apply directly to the Information Commissioner for a decision. Details of this procedure can be found on the ICO website: www.ico.gov.uk.

Generally, the ICO cannot make a decision unless you have exhausted the complaints procedure provided by the Local Government Boundary Commission for England.

Yours sincerely,

Karen Cleverly
Business Support Officer
Karen.cleverly@lgbce.org.uk
0330 500 1260

The Local Government Boundary Commission for England

INFORMATION SECURITY POLICY

1. INTRODUCTION

One of the LGBCE's greatest resources is the accurate and up-to-date information it relies upon on a daily basis to function.

We often take the information we use on an everyday basis for granted and forget it has enormous value as a business asset to ourselves and is also potentially valuable to criminals. It's therefore important that all LGBCE staff handle both electronic and paper data carefully to avoid security breaches.

It's important to remember that the result of information being handled in an unsecure way by LGBCE employees and Commissioners could result in:

- Financial Losses,
- Essential Business Data Loss,
- Damage to the LGBCE's reputation,
- Failure to meet the LGBCE's legislative obligations,
- The publication of Information not yet in the public domain, which becomes detrimental to the LGBCE.

This policy aims to outline how the LGBCE's data is securely managed and the steps that LGBCE staff can take to protect the organisations networks, databases, hard-drives and software.

This policy gives an outline of processes followed by the LGBCE. However if further information is required regarding ICT security issues, please refer to the following related Polices and Procedures;

- LGBCE's Personal Data Policy,
- LGBCE's Acceptable Use Policy,
- L!berata's Communications and Operations Management Policy,
- L!berata's Communications Network Security Policy.

2. POLICY BACKGROUND

The following basic information security principles have formed the basis for this Information Security Policy:

- Confidentiality – ensuring that information is accessible only to those authorised to have access

- Integrity – safeguarding the accuracy and completeness of information and processing methods

- Availability – ensuring that authorised users have access to relevant information as required

This Information Security policy has been formulated, taking into account the appropriate legislative requirements of:

- The Data Protection Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- ISO 27001 Best Practice Standards

The objectives of this policy are as follows:

1. To raise the awareness of LGBCE employees and Commissioners, regarding the organisation's responsibilities to ensure that risks to Information Security are managed.
2. To give LGBCE staff a fuller understanding of how information is managed through L!berata.
3. To inform employees how information can be securely managed, processed, created and stored in a logical way.
4. To ensure that staff are aware that only authorised employees have access to the LGBCE's technology systems and that access is granted proportionally to the each employee's position within the LGBCE.
5. To outline how all the LGBCE's technology assets (software programmes, databases, hardware, licenses, network and communications systems and portable equipment) are protected against loss, theft, abuse and misuse.
6. To ensure that all LGBCE staff and system users understand their responsibilities for the maintenance, protection, confidentially and integrity of the data they handle.
7. To ensure all external support agencies and service providers are aware of the LGBCE's information security policy and comply with the principals.

3. RISK MANAGEMENT

The management of Information Security is an on-going transitional process, which develops as new technologies and programmes are used by the

LGBCE and the organisations external contacts. To ensure the LGBCE manages information security risks, the Senior Management Team take responsibility for all foreseeable risks associated with Information Security through regular liaison with Liberata service providers and review of this and related policies.

4. LI!BERATA

As a small organisation with limited resources, much of the LGBCE's associated business functions are undertaken by Liberata. L!berata are 'back-office' service providers, who are contracted by the LGBCE to provided IT management and maintenance services at LGBCE's Layden House Office.

Below is a list of IT functions undertaken by L!berata for the LGBCE, however this list is not exhaustive and will change and develop over time. Such changes and developments will be recorded in regular reviews of this and related policies;

- Ensuring that at all times the LGBCE's IT systems are functioning to an optimum level.
- Undertaking regularly back-ups of all LGBCE's electronic files (including email).
- Ensuring that the LGBCE's files and computer systems are adequately protected against viruses, spyware, malware and external attack.
- Updating and maintaining the LGBCE's computer hardware and telephone equipment.
- Maintaining the LGBCE's main computer servers.
- Maintaining Data-Recovering systems to ensure the LGBCE's Business systems could be accessed if the Offices and Hardware at Layden House became inaccessible or unusable.
- Installing new software at the request of the LGBCE.
- Maintaining and updating existing LGBCE software.
- Providing a telephone and email advice services for queries and problems relating to IT hardware and software.
- Maintaining Internet and Intranet provisions at Layden House for the LGBCE and LGA group.

If you require any further information regarding the IT services provided by L!berata please call the L!berata help line on 8888 or view their intranet page at http://familyportal/sites/liberata/default.aspx?CatID=8cb4df0a-54f1-4581-8f73-d3a964e4e4aa .

Alternatively if you are experiencing a problem with your telephone, PC or office equipment and wish to log a fault please call OneCall on 3303 or send an email to onecall@local.gov.uk.

5. PERSONAL SECURITY SCREENING

5.1 Layden House

The LGBCE operates from a secure Office within Layden House. Employees and LGBCE Commissioners gain access to the LGBCE Offices through the use of individual security passes, identifying each user by their name and photograph.

The LGBCE offices are not directly open to the public and visitors should be accompanied by LGBCE staff members. If visitors are checking in at Layden House reception, an on-line booking should be made to keep reception staff up dated.

LGBCE employees should alert Layden House reception staff (dial '0') if unauthorised personnel are found within the LGBCE offices.

If LGBCE staff misplace their security pass they should report to Layden House reception as soon as they become aware that they do not have their pass. Layden House reception will then issue a replacement temporary pass as a short term measure. However If a member of staff have lost their security pass instead of just misplacing it, then arrangements should be made with facilities management to issue a replacement pass. This can be done by contacting Derek Young at the Layden House reception desk. Please dial '0' or email Derek at DerekYoung@liberata.com if you need to contact him.

5.2 HR Screening

When new staff are employed by the LGBCE, it will be the responsibility of L!berata's HR team to carry out background verification checks on all candidates. Contractors and third parties used by the LGBCE, will also be subject to verification checks which may be carried out by L!berata's HR services or by the agencies introducing the candidates.

Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as Data Protection or Freedom of Information**.**

As part of the recruitment process, new employees are required to sign and adhere to the LGBCE's Code of Conduct, which states that all policies and procedures will be adhered to.

6. INTRANET PORTAL

The LGBCE and other bodies within the LGA group currently have access to an intranet LGA Group Portal. This is displayed as the intranet Home Page. Through the home page a number of in-house services can be accessed, including the following;

- Layden House & Local Government Houses' Room Booking's facility.

- Hotel Bookings' facility,
- Visitor Registration,
- Taxi and Transport bookings' facility,
- Courier Bookings,
- Agresso Login,
- Maintenance requests and Facilities Management requests,
- A People Finder Directory

The above list is in no way exhaustive and the home page is being regularly updated with information and new services for LGA group staff.

Within the LGA group home page a separate portal can be assessed for the LGBCE and for L!berata services.

The LGBCE portal is restricted to LGBCE staff use only. The LGBCE portal includes the range of LGBCE policies and procedures, HR forms, LGBCE staff contact details and other vital information for the use of staff.

Access to external web pages is also available through the home page.

7. ELECTRONIC FILING;

All members of LGBCE have access to the shared drive (X-Drive), accessible at Layden House and all LGBCE staff can also access a personal drive, through 'My Documents'.

Currently within the X-Drive some files are restricted by password controls**.** Privileges to access these files, will only be allocated on a role-based model and as required, i.e. the minimum requirement for their functional role and only when needed. Those with privileges to access password controlled files, should keep all passwords secure at all times.

It is essential that ALL corporate documentation should be stored electronically on the X-Drive and that only personal documentation should be stored in 'My Documents'. This ensures that corporate documentation (including developing and draft documents) are accessible to all.

All LGBCE employees should be aware of what documentation they hold on in paper copy on their desks. It is good practice to ensure that all documents are cleared for their desks at the end of each day. However if this is not possible, special attention should be paid to sensitive or personal data, which needs to be stored securely and not left on desks over night.

To ensure information is stored in a logical and accessible way, LGBCE is currently undertaking a Records Management project to ensure the accuracy of data held in both electronic and paper forms, and to redesign its filling system for maximum efficiency. A Records Management policy will be produced at the end of this project. The Information Security policy will also be updated to bring it into line with the Records Management policy.

8. INFORMATION GOVERNANCE

The management of Information Security at the LGBCE is the responsibility of ALL staff and Commissioners. The following details how Information Security is managed as a corporate function.

8.1 Executive Responsibility

The Senior Management Team has responsibility for signing and endorsing information security polices, all supporting polices and any significant changes required.

The L!berata IT team has responsibility to manage the supporting information systems and ensure that information is protected and maintained to the highest standard.

Members of staff are responsible for the operational security of the information systems they use. Each user should comply with the security requirements that are currently in force, and ensure the confidentiality, integrity and availability of the information they use. LGBCE staff should adhere to a number of LGBCE policies to reach this goal, including, but not exhaustively the LGBCE's Data Protection and Personal Data Policy and the ICT Acceptable Use Policy.

8.2 Senior Information Risk Owner (SIRO)

The LGBCE Senior Information Risk Owner (SIRO) is currently the Director of Reviews who is assisted in this role, by members of the Senior Management Team. The overall responsibility for appointing the LGBCE's SIRO rests with the Chief Executive.

It is the SIRO's responsibility to ensure that the Senior Management Team understands and own the information security and information risk policies. The SIRO provides written advice to the Senior Management Team on internal controls relating to information security and risk. The Senior Management team has overall responsibility for ensuring the implementation and communicating of information security requirements across the organisation. The SIRO has responsibility for monitoring the communication and implementation of the Commission's information security policies, the identification of all major information assets and the maintenance of a central information risk register.

8.3 Information Asset Owners (IAO)

The Business & Committee Services Manager has been appointed by the Chief Executive as the LGBCE's Information Asset Owner (IAO). The IAO will be assisted by the Review Managers and members of the Implementation team in this role. The IAO has a responsibility to address any risks to information and to ensure that information is used within the law.

8.4 Departmental Records Office (DRO)

The Business Support Assistant currently acts as the LGBCE's Departmental Records Officer. The DRO is responsible for the transfer of paper records to the National Archive.

8.5 L!berata Service Delivery Manager

The L!berata Service Delivery Manager is responsible for all aspects of IT including the provision and maintenance of IT equipment. Areas of responsibility include management of all technology assets comprising the technical architecture, liaison with and management of 3rd party technical support and managed service providers.

The Service Delivery Manager is directly responsible for ensuring the security and integrity of the network systems and maintaining access controls to information systems and databases, supported by both the local area network, (LAN), and the MPLS managed network provided by the contracted Internet Service Provider (ISP).

The Service Delivery Manager is also responsible for enforcing access rights to restricted levels of the business classification scheme, to maintain the security and integrity of data contained within the electronic files maintained on the X drive.

Currently the LGBCE's Service Delivery Manager is Winston Andrews (email WinstonAndrews@Liberata.com, mobile 07884116018).

8.6 Data Protection and Freedom of Information Officer

Responsibility for compliance with Data Protection and FOI legislative requirements and ensuring awareness across the LGBCE rests with the Senior Management Team. However Bola Ojoye Implementation Team Officer directly deals with all Data Protection and FOI requests and ensures the LGBCE complies with all targets set by the ICO (Information Commissioners Office). For further information regarding the LGBCE's FOI procedures and processes, please refer to the LGBCE's FOI policy.

8.7 LGBCE Employees

Line management is responsible for ensuring that all employees, both permanent and temporary are familiar with the LGBCE's policies and procedures in relation to information management, security and authorising appropriate access rights to corporate data and information systems.

In turn, all users of the LGBCE's information systems are responsible for managing their own data to ensure it is maintained in compliance with internal policies and procedures and that they abide by security controls implemented for the protection of information and security of the information systems.

9. CONTROL OF ASSETS

As the LGBCE contracts all Information Assets directly from L!berata both the Business Team and the L!berata Service Delivery Manager will categorise and record all Information assets such as PCs, to enable appropriate management and control. The asset inventory should include all information necessary in order to recover from a disaster.

Asset management of ICT equipment has been established so that effective tracking, security and management of these assets can ensure continuity of ICT equipment. The Business Team will ensure that inventories of these items are properly maintained by conducting regular audits of equipment. New equipment will be added to the asset management system before being issued to members of staff.

10. ACCESS CONTROLS

10.1 User Authentication and registration

All LGBCE staff and Commissioners will have a unique identifier (user name) and an authentication method (password) to access the information systems of the Commission.

Each individual user must be responsible, and therefore accountable, for the access credentials provided to them, including user accounts, passwords, security passes and any PIN numbers that they are given to access restricted folders. It is each user's individual responsibility to ensure their access credentials are adequately protected from loss or disclosure.
All managers must promptly notify HR and ICT when new members of staff or new Commissioners require access to the system and when members of staff or Commissioners leave the LGBCE.

10.2 Password Control

Upon commencing employment with the LGBCE, all employees will be given a user name and password for access to the network via their desktop PC.

An user name and password pair can be likened to a key set issued to an individual. These are signed out for their use to access resources for which they have been granted access, and for no other purpose. The sharing of individual passwords or user names is not permitted, except in cases of urgent necessity. User names should also be treated as confidential and only revealed, upon request, to authorised individuals; e.g. system administrators or help desk employees trying to resolve a support issue.

An account expiry date must be set for all temporary accounts. The expiry date must be set for the leaving date of the temporary employee. Temporary employees should be made aware of this expiry date in order for them to

request extensions if necessary. Requests for extensions must be validated by Managers.

It is the responsibility of each employee to ensure that their user name and password remain confidential at all times

Here are some tips to ensure when choosing or changing Passwords;

- a minimum of 8 characters
- a mixture of upper and lower case alpha, numeric and ideally symbol characters
- not part of a recognisable word or phrase or network user name
- not stored either on paper or electronically where it can be accessed by other personnel

System users are prompted every 30 days to change their password which must be unique for 5 changes but, can change their passwords voluntarily by pressing **CTRL+ALT+DEL keys simultaneously and selecting the "Change Password" option.**

In the event of forgetting a password or inputting it incorrectly, users will have 5 attempts at accessing the system and their user account before they are automatically locked out. In such circumstances the account can only be re-enabled by L!berata through contacting OneCall.

Where problems are experienced in accessing the network all users are asked to contact the **One Call Help-desk on ext 3303.**

Where an employee leaves their desk unattended they should either log off the system, if away from their desks for a prolonged period or lock their desk-top by pressing **CTRL+ALT+DEL keys simultaneously and choosing the option "Lock Computer"**

Desk-top PCs are set to lock automatically after 15 minutes, if not in use, and can only be re-enabled by re-entering a user name and password.

Mangers should ensure that appropriate exit procedures are carried out with outgoing employees or contractors before departure, including:

- A thorough housekeeping takes place of outgoing employees or contractors data before they depart;
- The IT Help Desk are informed of their departure and requested to disable or delete all associated accounts.
- Any access credential the user may possess, such as security passes, are handed in.

10.3 Data Back-Up

Back-ups of essential information and software, used by the network such as configuration files must be taken on a regular basis by the L!berata ICT Team, according to a defined cycle, to ensure that, in the event of an emergency, the information or software can be restored within critical timescales.

All commission data is stored centrally on servers located in a secure environment with limited access to authorised L!berata ICT personnel only. All backup media is held off site.

If a data restore is required, this is requested via the ICT helpdesk. Restores cannot be performed on data that was created and deleted on the same day, as no backup would have been performed in the time frame to which the creation and deletion took place.

10.5 External Support Agencies

As already stated the LGBCE outsources its IT support to L!berata. Support arrangements and service levels agreements are reviewed regularly at Contract Management Board meetings and to which L!berata must adhere.

Before entering a contractual arrangement all 3rd party agencies (such as L!berata) will be invited to partake in a risk assessments with the Senior Management Team. To ascertain the adequacy of the 3rd party development and support environments for maintaining the security and integrity of the LGBCE's corporate data, applications and network systems.

10.6 Firewalls

The LGBCEs' IT network systems are protected from the public domain by a series of firewalls to ensure that access from the Internet is restricted to permitted traffic only.

Annual penetration testing and vulnerability assessments are undertaken by an independent external specialist agency. To provide ongoing reassurance as to the security of networks and the effectiveness of firewalls, against the threat of hackers, unauthorised access and other security breeches.

10.7 Viruses

All PCs and servers are protected by McAFee VirusScan. This is controlled and monitored by L!berata and reports can be produced if required to capture data of any virus intrusion.

Email is scanned before it enters the LGBCE's network system and then again as it is placed in the user's mailbox, to ensure virus patterns are kept up

to date. If a user is suspicious of an email, they should contact L!berata on 8888, immediately and not forward the email to anyone

To account for newly detected viruses the ICT systems download a new virus signature file daily. The AntiVirus software cannot be disabled by any member of staff other than a network administrator.

Data that has come from an external source which cannot verify that it has been scanned for viruses must be scanned by a member of the L!berata IT Team prior to transferring to a network PC.

10.8 Portable Equipment Security

All users must ensure that PC equipment is not moved from the designated desk to which it is assigned, other than by a member of the L!berata ICT Team. If you require your PC equipment to be moved, please contact OneCall on 3033.

Users are advised to take the following precautions when taking portable equipment such as Laptops and Blackberries offsite:

- to take care of the equipment to protect it against theft, particularly while travelling

- not to leave it unless absolutely necessary in a parked vehicle, and then to lock the laptop in the boot of the car

- not to leave it unattended in, for example, a train luggage rack

- to ensure if working offsite, the equipment is always kept within view

- ensure security of data while working, e.g. ensure no-one can view your screen and view sensitive data.

- Under no circumstances should Electoral Register Information be held on a laptop or blackberry. Electoral Register information should only ever be held on static computers within LGBCE's secure offices, and are subject to a password control.

- Under no circumstances should memory sticks be used to file LGBCE business files. This rule does not apply to any information required for public presentation documents, such as PowerPoint presentations and public consultation literature, which can be uploaded to memory stick at SMT's discretion.

- All LGBCE staff should note that the loss of portable PC equipment could lead to a charge being made against the authorised user to replace the loss.

10.9 Monitoring Access

LGBCE Employees should be aware that L!berata ICT may operate non-intrusive exception monitoring of employees' use of L!berata's computer resources, including email and Internet use. This means that reports may be generated where inappropriate use is detected. There is no direct monitoring or intervention, unless a genuine possibility of inappropriate use has been raised through automated exception reporting, disciplinary proceedings or an employee complaint.

If action is required as the result of inappropriate use of computer resources, then the issue will be referred to the relevant Line Manager for remedial action to be taken which may include disciplinary action up to and including dismissal for gross misconduct, in appropriate cases.

The Regulation of Investigatory Powers Act 2000 permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

The LGBCE has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

11. SOFTWARE AND LICENSING

The L!berata ICT Team will ensure that all information products are properly licensed. Computer Software can only be purchased and installed by the L!berata ICT Team; under no circumstances is computer software to be purchased or installed by LGBCE staff.

11.1 Requests for Software

Software can be requested by LGBCE staff, but proper justification from the requester and sign off by the line manager must take place. Upon justification of software, purchase, testing and installation will take place by the L!berata ICT Team. Requests for new software should be made to the OneCall helpdesk on 3033, a software purchase form will then need to be filled in and signed by a member of SMT before the equipment is purchased.

11.2 Shareware, Freeware and Screensavers etc.

Shareware, freeware, screensavers, music files and games are bound by the same policies and procedures as all software; no user may install any free evaluation software. No software is to be downloaded from the internet without the written permission of the L!berata ICT Service Delivery Manager.

11.4 Fonts

Fonts are bound by the same policies and procedures as all software within the Organisation, and are not to be downloaded or installed without prior discussion with the L!berata ICT Service Delivery Manager.

12. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENACE

Information systems include operating systems, business applications, off-the-shelf products, services and user-developed applications. The design and implementation of the information systems supporting business processes are crucial for security. Security requirements should be identified and agreed prior to development and/or implementation. In particular, an assessment of the impact levels of the data to be held within the system should be made as this will inform the levels of security and access control required of the system. These matters should be discussed at an early stage with the L!berata ICT Team.

12.1 Specification of Business Requirements

In recognition of the above, LGBCE staff must ensure specifications for business requirements for new, existing and enhanced business applications address requirements for security controls such that:

- security requirements are identified, documented and agreed as part of the overall business case justification for investment in a project
- system requirements for information security and processes for implementing security are integrated in the early stages of all development projects at the design stage.
- software packages purchased are evaluated against clearly defined security requirements for both automated and manual controls

13. Audit and Reporting

The LGBCE will consider information risk as part of it’s Corporate and Operational Risk Registers. Management of risk through these Risk

Registers will be overseen by the Senior Management Team and reported to the Commission's Audit Committee and the Commission as a whole.

The SMT in conjunction with the designated SIRO and Risk Managers, will conduct regular reviews of Information Risk as part of it's Risk Management program. As part of these reviews, the effectiveness of the this policy and any related procedures and policies will be assessed.

14. Policy Review

The Information Security policy will be reviewed at least on an annual basis by the LGBCE SMT.

Issues to be considered as part of the review include:

- changes to the technical infrastructure
- the results of vulnerability and risks identified within the Corporate Risk Register.
- records provided by L!berata ICT, of viruses detected, damage caused and impacts of unauthorised intrusions to the network
- advice received from external agencies.
- advice received from external consultants, such as penetration testing results, major firewall changes etc.

A summary of the findings and recommendations of the review will be incorporated in revisions of this Information Security Policy, ratified and approved by the Senior Management Team.

The
Local Government
Boundary Commission
for England

Information Management & Security Policy

Document status

Abstract	This document outlines LGBCE's approach to information management & security. It details the overall aims and principles by which the Commission seeks to ensure that information risks are managed appropriately and proportionate protective controls are in place.
Date Issued	09.03.2016
Version and status	Final V1.0
Revision Frequency	Yearly
Owner	Jolyon Jackson
Author	Alex Palacky
Contributors	
Protective marking	

Document revision

Version	Date	Revised by	Purpose of issue	Summary of changes
v0.1		Alex Palacky	First Draft	Revision and amalgamation of existing Information Management & Information Security Policies
V1.0	09.03.2016	Alex Palacky	Updates as per A&R Committee feedback	

Document distribution / approval

Name	Title	Date	Purpose
Jolyon Jackson	Chief Executive		For comment
Audit & Risk Committee		22.02.2016	For authorisation

Contents

1. Introduction

1.1 Purpose

The purpose of this policy is

- To ensure that information is accessible only to those authorised to have access
- To safeguard the accuracy and completeness of information and processing methods
- To ensure that authorised users have access to relevant information as required
- To ensure that the organisation can operate effectively and efficiently on a day to day basis
- To ensure that in the advent of an incident affecting the organisation's information systems or content, LGBCE has adequate Business Continuity processes in place to restore the corporate memory
- To ensure compliance with information law governing the management of public records

1.2 Scope

This policy provides a framework for the management of information security in all its formats throughout the LGBCE. It applies to

- Anyone with access to the LGBCE information systems. This includes full and part time staff, Commissioners, contractors, temporary workers and visitors.
- Any systems attached to the LGBCE computer or phone networks and any supplied systems.
- All information processed by LGBCE in line with its operational activities, regardless of if it is processed electronically or in paper form, any communications sent to or from the LGBCE and any information held on systems external to the company network.
- All external parties that provide services to the LGBCE in respect to information processing facilities and business activities.
- Principle information assets including the physical locations from which the LGBCE operates.

1.3 Related Policies, Legislation & Standards

This document highlights the policies followed by the LGBCE specific to Information Management & Security and is written to work in conjunction with the following LGBCE policies:

- Personal Data Policy
- Acceptable Use Policy
- IT Security Policy
- Business Continuity Plan
- Incident Reporting Procedure – Information Security

The effective implementation of this policy ensures that the LGBCE is in a position to meet the legislative requirements of:

- The Data Protection Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Health & Safety at Work Act 1974
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Political Parties, Elections and Referendums Act 2000
- Environmental Information Regulations 1992 and Amendment 1998
- Public Records Act 1958
- The Disposal of Documents Order 1925
- ISO 27001, 15489, 23081, 18492, 27002 and BS 10008:2008

2. LGBCE Responsibilities

The LGBCE shall undertake the correct processes to ensure the following.

2.1 Employment
All contracts of employment address information security requirements in order to protect information that is held in confidence. New staff are also subject to HR screening to ensure positive background verification checks. Any specific security roles or responsibilities will be outlined in the job description.

Managers are responsible for ensuring correct exit processes take place to minimise the risk of a breach of information security.

Information Management & Security Policy training is covered in all new staff inductions.

2.2 Access Controls
Access controls are in place to ensure that only authorised staff can access information. The LGBCE operates from a secure office which requires a personalised security pass to access. Each employee has their own individual user name and authentication method to access the Commission information systems and the server control level is monitored by the Service Delivery Manager (SDM). All confidential hard copy files are securely stored and soft copy files are password protected as necessary.

Each user is responsible and accountable for their own access controls. This includes security passes, passwords, pin numbers and user account details. The sharing of access controls is prohibited except in cases of urgent necessity, and should be updated if this has happened.

2.3 Asset Security
In order to minimise losses or risk of damage an asset register is managed by the Business Team. This includes all information necessary to recover from a disaster. Audits are carried out to ensure integrity of the information.

2.4 Information Risk Assessment
A regular assessment of the working environment is undertaken by the Senior Management Team and the results are captured on the corporate risk register. As part of these assessments, the effectiveness of this policy and any related processes and programs are also reviewed. Information risks are reported to the Commission's Audit & Risk Committee and the Commission as a whole.

2.5 Security Incidents and Weaknesses
Information security incidents must be reported to the SIRO so it can be recorded, investigated and ideally remedied. It is important for future proofing that the cause is defined and the impact and effect on the LGBCE is recorded. Refer to the Incident Reporting Procedure for information on how to report a security incident.

2.6 Network Protection
The LGBCE's PCs and servers are protected by McAfee VirusScan. It is controlled by our 3rd party IT Company who can produce reports of any virus intrusion. This software can only be modified or disabled by a network administrator.

The LGBCE's network systems are protected by a series of firewalls to ensure that access from the internet is restricted to permitted traffic only. Annual penetration testing and vulnerability assessments are undertaken to ensure effectiveness of the firewalls.
All employees are advised to take precautions when removing IT equipment from the office (e.g. taking a laptop or iPad to an external meeting) to ensure security of the information on the device.

It is expected that anyone with access to the LGBCE information systems (including full and part time staff, Commissioners, contractors, temporary workers and visitors) will take all the necessary precautions to minimise the risk of a network information breach. This includes but is not limited to:

- Only logging into secure Wi-Fi networks
- Keeping unique logins and passwords safe
- Ensuring hardware & hard copy files are stored and transported safely
- Using supplied hardware and software for its intended purpose
- Checking with the Service Delivery Manager before downloading third party applications
- Checking email recipients are correct and correctly listed (to, cc and bcc) before sending sensitive information

2.7 Secure Communications
Secure communication processes are in place to ensure the secure transfer of all information whether it be via telephone, fax, email or letter correspondence.

2.8 Business Continuity and Disaster Recovery Plans

The LGBCE has a Business Continuity Plan (BCP) in place so that in the event of a disruption to the information services it is possible to activate the relevant business contingency plans until the affected services have been restored.

3. Staff & Commissioner Responsibilities

3.1 Executive Responsibility

The Operational Management Team (OMT) are responsible for signing and endorsing information management and security policies, all supporting policies and any significant changes required. They are also responsible for ensuring the implementation and communication of information management and security across the LGBCE.

3.2 Senior Information Risk Owner (SIRO)

The SIRO is currently the Finance Director who is assisted by the OMT. The responsibility of electing the SIRO rests with the Chief Executive.

The SIRO is responsible for ensuring the OMT understands the Information Management & Security Policy. They are also accountable for monitoring the communication and implementation of the Commission's information security policies, the identification of all major information assets and the maintenance of a central information risk register.

3.3 Information Asset Owners (IAO)

The IAO is currently the Business Team who is supported by the Review Managers. The responsibility of electing the IAO rests with the Chief Executive.

The IAO is responsible for addressing any risks to information and to insure information is used within the law.

3.4 Service Delivery Manager (SDM)

The SDM is currently the Project Officer who is supported by the Business Team. The responsibility of electing the SDM rests with the Chief Executive.

The SDM is responsible for all aspects of IT for the LGBCE including management of our 3rd party technical support. The SDM is directly responsible for ensuring the security and integrity of the network systems and maintaining access controls to information systems and databases supported by both the local area network and the MPLS managed network provided by the contracted Internet Service Provider. They are also in charge of enforcing access rights to restricted levels of the business classification scheme in order to maintain the integrity of data contained within the electronic file systems.

3.5 Data Protection and Freedom of Information Officer

Responsibility for compliance with Data Protection and FOI legislative requirements and ensuring awareness across the LGBCE rests with the OMT and is supported by the Business Support Officer. For further information please refer to the LGBCE's FOI Policy.

3.6 All LGBCE Employees
Line Managers are responsible for ensuring that anyone employed by the LGBCE who has access to company information are familiar with the LGBCE's policies and processes in relation to information management and security.

3.7 Commissioners
Commissioners are responsible for complying with the LGBCE's policy on Information Management and Security when using LGBCE equipment (i.e. iPad's or laptops, Wi-Fi and networks) and when in possession of LGBCE information (e.g. meeting agenda's and papers, LGBCE contact details etc.) They must inform the SIRO if there has been a breach of this policy, for example if they have logged into an unsecure network using LGBCE property, or have lost LGBCE property containing company information.

In turn, all users of the LGBCE's information systems and responsible for managing their own data to ensure it is maintained in compliance with internal policies and processes.

The Local Government Boundary Commission for England

In Association With

L!berata Human Resources

L!BERATA
outsourcing work flows™

HUMAN RESOURCES • HUMAN RESOURCES

Personal Data Policy

Introduction

The LGBCE is a small organisation that uses Liberata services to provide a number of 'back-office' services, such as Human Resources, Facilities Management, ICT provision and maintenance. As both routine and personal data concerning LGBCE staff, is managed and stored by Liberata as part of their contract with the LGBCE, this policy has been produced taking into account Liberata's Data management policies and procedures.

Within this policy the term 'Liberata' is used to define the company's functions as a sub-contracted HR facility and ICT provider for the LGBCE.

Who does this Policy and Procedure Apply to?

This policy and procedure applies to all LGBCE employees regardless of their type of employment contract e.g. temporary, fixed term etc and also includes contractors who are providing services, agency workers and trainees on vocational or work experience schemes. This policy and procedure is non-contractual and may be amended or departed from at the LGBCE's discretion.

What is the Purpose of the LGBCE's Personal Data Policy?

The LGBCE is committed to ensuring that the processing of data (such as addresses, phone numbers or any other information that could identify an individual), which concerns its employees, its clients or customers, is carried out with the appropriate safeguards for their rights and freedoms and that the data is not processed in an unfair or unlawful manner.

The LGBCE will obtain records and process personal data in accordance with the principles set out in the Data Protection Act 1998. A summary of the data protection principles is given in the section below, as is an outline of employee's rights of access to the information held about them by the LGBCE. Personal data refers to any information, whether held on computer or in manual filing systems, about an individual or from which an individual can be identified.

The Act grants employees certain rights to have access to information held about them and to correct inaccurate data. In some circumstances employees may also object to the processing of personal data or prevent certain information being held or being used in particular ways. The Act aims for a balance between the need of an employer to keep and process personal data and the right of an employee to have his or her private life respected.

The personal details of any employee or contractor will not be disclosed to anyone outside the LGBCE or L!berata, without the permission of the individual concerned, other than an employment reference, unless a disclosure is required by law. All personal information will be held by the LGBCE in secure environments and protected from unwarranted disclosure. Equally, no employee is permitted to disclose personal data held on others to

any individual or organisation outside the LGBCE or to use personal data for their own purposes.

In this policy the word “processing” means any action involving data – computerised or manual - including obtaining information about an employee or customer, storing or using such information, and disclosing information to a third party.

The word “data” means, in broad terms, any information or opinions that Liberata or the LGBCE has obtained or produced concerning, an employee or customer. Customer data can include the names, addresses and contact details of clients or data such as electoral rolls that is being analysed by the review teams.

Breach of this Policy and Procedure will be viewed as very serious, and may lead to disciplinary action up to and including dismissal in the case of gross misconduct. In addition, an employee may be criminally liable if s/he knowingly or recklessly obtains accesses or discloses personal data about fellow employees, clients or customers without the authority and consent of Liberata HR or the LGBCE. There may be certain exceptions to this policy and employees should also read this policy in conjunction with the LGBCE's Whistleblowing Policy and Procedure.

This Data Protection & Personal Data Policy has been designed to reflect the guidance set out in the draft Code of Practice issued by the Data Protection Commissioner in response to the Data Protection Act 1998.

What is the purpose of the Data Protection Act?

The Act is concerned with protecting the privacy of individuals and requiring transparency in the use of information. It sets out principles by which personal data should be used, which state that personal data must be:

- fairly and lawfully processed
- processed for limited purposes and not in any manner incompatible with those purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than necessary
- processed in accordance with individuals’ rights
- retained securely
- not transferred to countries without adequate data protection laws

This applies not only to employees but also to our clients and customers.

In accordance with the above principals, the LGBCE will hold records and process personal data in the following ways –

Personal data will be obtained, held and recorded fairly and lawfully;

Personal data will be held only for specified and lawful purposes, and will not be further processed in a way which is incompatible with the purposes;

Personal data will be adequate, relevant and not excessive in relation to the purpose(s) for which it is held;

Personal data will be accurate and, where necessary, kept up to date;

Personal data will not be held longer than is necessary for the purpose(s) for which it has been obtained;

Personal data will be processed in accordance with the rights of the employee for access to the data;

Appropriate measures will be taken to avoid unauthorised or unlawful processing of personal data, and against accidental loss, destruction or damage to personal data.

Access to Personal Data

You are able to access your personal data held on the HR database via L!berata. Please ensure you keep this information accurate and up to date. Your personal file will retain the data you provided with your application to join the Commission as a record of your employment history, qualifications and related matters. Information related to your pay, pension, training, performance, and attendance will also be kept and updated for the purposes of resource management. Copies of internal correspondence sent to you, or by you, will also be kept as a central record by L!berata.

If you wish to request information you should contact the L!berata HR Team on 0207 296 6198. In accordance with L!berata's policies, the reasonableness of your request will be judged on the basis of the personal data requested and the frequency with which that data is updated. If your request is granted, the information will be provided at the earliest possible time but in any case not later than 40 days from receipt of the request.

Where disclosing data to you will inevitably involve identifying a third party, your request can be refused unless the third party has consented to the disclosure or it is reasonable to comply with the request without their consent. Matters of a particularly sensitive or private nature relating to a third party would not normally be disclosed. It is not normally regarded as reasonable to disclose references of ex-employers, on the grounds of a duty of confidentiality, unless the ex-employer has given explicit consent to do so. Internal references given in confidence for the purposes of education, training or employment are also exempt from disclosure.

If you have concerns on any matters relating to your access to, and the processing of, personal data, you should raise this informally with your manager or a member of the L!berata HR Team.

Where is information about employees held within Liberata's HR?

The Liberata Human Resources Department for the LGBCE holds a paper based personal file for each LGBCE employee. Some LGBCE managers may also hold information on the individuals within their teams to enable them to lead effectively e.g. copies of most recent performance appraisals and objectives for the current year etc. In addition to paper based files, the following computerised records systems are also used to store and process personal data:

- the Liberata human resources administration system, known as SAP
- the Liberata payroll system
- the LGBCE pensions system
- In addition, monitoring of the use of Liberata's telecommunications and ICT equipment also takes place (refer to the LGBCE's ICT Security Policy and procedures).

Does Liberata operate any key principles in managing LGBCE employees' data?

Yes. Liberata will not process any data relating to any LGBCE employee without their consent unless the processing is necessary:

- for the performance of an employee's contract of employment with the LGBCE or the LGBCE entering into a contract of employment with him/her
- to enable the LGBCE or Liberata to comply with their legal obligations
- to protect the employee's vital interests
- is warranted to protect the legitimate interests of the LGBCE or Liberata

Certain types of information are classed as 'sensitive personal data' and to hold this the LGBCE requires your consent, gained either through a specific request or through your employment contract. Data of this kind relates to information on: race, religion or belief; political opinions; union membership, sexual life; the commission or alleged commission of any offence; and physical or mental health or condition. Data concerning employees which is considered 'sensitive personal data' will not be processed without their explicit consent, unless the processing is necessary:

- to enable the LGBCE to comply with its legal obligation in connection with employment of staff, examples include ensuring the health, safety and welfare of staff; ensuring the equality of opportunity or treatment of staff; or selecting competent employees
- to protect their vital interests or those of another person and consent cannot reasonably be obtained
- the individual has already made the information public

- for the purpose of or in connection with legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights
- for medical purposes and is undertaken by a health professional (or someone owing an equivalent duty of confidentiality)
- for the purpose of identifying or keeping under review the existence or absence of equality of opportunity

The LGBCE or Liberata will, wherever reasonably practicable, except in the processing of personal data supplied by employees for Human Resources purposes, seek employees' clear written consent to the processing of data (including sensitive data). Employees have the right to withdraw their consent at any time by writing to their Liberata Human Resources Administrator or their manager.

Where data is disclosed to a third party, the LGBCE and Liberata will inform the employee of the fact and reasons for the disclosure, and the nature of the data disclosed, unless this would prejudice the outcome of certain legal proceedings as specified within the Act.

Liberata will take appropriate technical and organisational measures against accidental loss or destruction of, or damage to, personal data.

At all times, the LGBCE and Liberata will operate their procedures within the principles of the Data Protection Act.

The Commission will seek to eliminate irrelevant or unnecessary personal data from its records and to retain records for no longer than is appropriate for each type of data. The L!berata HR Manager – is responsible for ensuring that the Commission's employment practices and procedures comply with the Data Protection Act.

Who is responsible for managing data protection within Liberata and the LGBCE?

Various people hold responsibility for data protection within Liberata, including the following:

- The Liberata Data Protection Controller - has overall responsibility for determining the purposes for which any personal data is to be processed. This person is also responsible for investigating complaints made by LGBCE employees regarding Liberata's management of personal data.
- The Liberata National Data Protection Leader – is responsible for developing and monitoring the Liberata Data Protection Policy and Procedures. Changes to this policy will impact on the LGBCE's Data Protection and Personal Data policy.
- The Liberata HR Advisor for the LGBCE also acts as a Data Protection Co-ordinator and is responsible for providing advice, and giving guidance on data protection matters to all LGBCE employees. They

are also responsible for referring relevant matters to the Liberata Data Protection Controller where necessary.

Within the LGBCE the Senior Management Team are responsible for managing and assessing data protection issues and will review this policy on a regular basis

In addition, all employees have a responsibility to familiarise themselves with the requirements of this policy, and associated policies and procedures, and to adhere to these at all times.

What responsibilities do employees have with regard to data protection?

Employees have the following key areas of responsibility:

- All employees should ensure that the personnel record of their home address, phone number, and other contact information, held by L!berata on behalf of the LGBCE, is always up to date. This requirement also applies to bank or building society details so that salary payments can be made correctly by L!berata's Human Resources Staff. Employees should ensure that any changes to their personal details are notified to the Liberata Human Resources Administrator either directly or via their manager.
- To apply the data protection principles to all personal data they process in the course of their duties. Particular attention must be given to the handling of very sensitive data, such as electoral registrars, research documents and any other information that could be classed as personal or confidential. It is essential that sensitive data, such as electoral registers, are never passed onto third parties. Please read the LGBCE ICT Security Policy for further guidance on safeguarding the LGBCE's information assets or consult your manager for further advice

Can an employee view the data held about him/herself?

Yes. Employees have the right to:

- be informed whether data which concerns them has been or is currently being processed, the source of the data, to know what the data consists of, why it is being processed and to whom it has been, or may be, disclosed
- receive a copy of certain data held about them

Some information is exempt from access by the individual and this information includes:

- any personal data which could prejudice the prevention or detection of a crime, the apprehension or prosecution of offenders, or the collection of any tax or duty
- business forecasts and plans

- where the sharing of personal data might influence the outcome of a negotiation
- Confidential references given or received by Liberata on the LGBCE's behalf.

How does an employee arrange to view data held about him/herself?

An access request can be made by anyone who believes that data is held about them e.g. prospective, current, or past employees or unsuccessful interviewees. The LGBCE or Liberata may ask for information that helps the LGBCE or Liberata to locate the records e.g. dates of employment or some form of identification to ensure that information is only given to the person entitled to it.

There may be some information relating to an individual that may not be disclosed. In such instances, the LGBCE or Liberata will endeavour to release as much information as possible, without enabling any third party to be identified, even if that information actually relates to the third party as well as the employee.

The process for viewing data held by Liberata on behalf of the LGBCE, about oneself is as follows:

- The employee directly writes or e-mails his/her respective Liberata Human Resources Administrator requesting to see his/her personal data under the provisions of the Subject Access Rights of the Data Protection Act 1998. Requests can also be sent to the employees' manager, who will then forward on the request to the Liberata Human Resources manager.
- the Liberata Human Resources Administrator will print the employee's personal record from SAP and LGBCE Pensions and forward this with any other data relating to the employee giving details of why it is being processed, the source of the data and to whom it has been or may be disclosed and/or arrange a mutually convenient time for the employee to visit the Human Resources department to view his/her paper based personnel file, including any documents held by the employee's manager. This will be actioned by the Liberata Human Resources Administrator as soon as is reasonably practicable and in any event within forty days of receiving an access request
- The employee should check the record and either make any necessary amendments and return the information or notify the Liberata Human Resources Administrator in writing that the form is accurate. If copies of any documents held on the employee's personal record are required by the employee, s/he should advise the Liberata Human Resources Administrator at the time of viewing the record, or in writing if required at a later date.
- the Liberata Human Resources Administrator will make any necessary changes to the record and either send an amended copy of the computerised record, or arrange for the employee to view his/her amended paper based record

- the employee should re-check the record at an agreed date ensuring that any changes have been carried out and notify the Liberata Human Resources Administrator in writing that the information is accurate

What information does the LGBCE disclose about its employees?

In some instances, the LGBCE has a legal obligation to disclose personal data about its employees and, in certain circumstances it may not make the employee concerned aware of such disclosures e.g. where it may prejudice a criminal or tax investigation. For commonly experienced requests from a third party requiring disclosures such as employment reference requests, mortgage reference requests etc. Liberata will inform the individual concerned prior to releasing the data. Records will be kept of all such disclosures on an individual's personal file.

Why is the Data Protection Act important in relation to our clients and customers?

In addition to our legal obligations under the Data Protection Act, data protection is also an important part of our relationship with our clients and customers for the following reasons:

- our commitment to providing a quality service means all aspects of that service, including data protection
- delivering client satisfaction is an essential part of everyone's job
- our compliance and commitment to data protection enhances our reputation

Examples

The following are for example only and are not meant to be a definitive list of the types of request that may be received. Where an employee has any concern or doubt about whether or not data may be disclosed, s/he should discuss this with his/her manager before releasing any data.

- **An individual asks to see all of his/her information**. Ask for the request to be made in writing suggesting that it would be helpful to provide the relevant reference number (if there is one) or context or nature of the records to be searched and explain that Liberata/LGBCE has 40 days to respond, from the date of receipt of such a request. .
- **Someone claiming to be a spouse/partner telephones to ask for information.** Explain you are unable to give out personal information. Ask for the individual concerned to telephone in person or write in with an information request.
- **A building society telephones and requests payroll information.** Most banks and building societies use an authorisation form. If a form has not been received, ask for the request to be made in writing, or by fax on business stationery e.g. headed paper
- **The police want information about an address.** Most public bodies ask for details on business stationery by letter or fax. In an emergency,

they may telephone in which case you should pass the call on to your manager.

What other actions can employees take to ensure data is protected?

Most actions are common sense, but the following may be helpful:

- follow the procedures laid down in the LGBCE's Information Security policy.
- ensure that any paper based documents that contain personal details are shredded rather than disposed of in office waste paper bins.
- take reasonable precautions to ensure that non-LGBCE employees, or unauthorised LGBCE employees, cannot see personal information e.g. do not leave documents on your desk or screen when your working area is not attended.
- Ensure that information kept is relevant, necessary and not kept for longer than necessary. There are both statutory and our own requirements that we need to adhere to, in terms of how long data must be stored. The LGBCE is currently producing an up to date Records Management and Record Retention Schedule, which will details how long documents should be stored for and how files should be managed.
- If you want to write to, or telephone a colleague at home and have not been given consent to contact them out of hours, you should contact the L!berata HR Team who will make appropriate arrangements for you to do so whilst preserving the confidentiality of your colleague(s).

Remember: the law holds the individual personally liable for any breaches by an individual.

The LGBCE is now registered with the Information Commissioner for England and adheres to all set principles and practices. A copy of the registration can be obtained by contacted Bola Ojoye (Implementation Officer). General Information regarding Personal Data legislation can be found from;

The Information Commissioner
Tel: 01625 545745
Web site: www.informationcommissioner.gov.uk