



Information Security Programme

Information Security Policy

This document is issued in the strictest business confidence.

It should be read in conjunction with a number of other supporting and complementary documents.

Further information and inquiries should be made to:

Brian Durrant
CEO
London Grid for Learning
CI Tower
St Georges Square
New Malden
Surrey KT3 4HG

T: 020 8408 4466
F: 020 8408 6014
E: brian.durrant@lgfl.org.uk

Ray Collins
Consultant
London Grid for Learning
CI Tower
St Georges Square
New Malden
Surrey KT3 4HG

T: 07860 783 984
F:
E: ray.collins@lgfl.org.uk

LGfL - Information Security Policy - 2010 - PUBLIC

Contents

Contents	2
Version Control.....	3
Introduction.....	4
Security policies - management direction.....	4
Risk assessment and mitigation.....	5
Organisation / governance of information security.....	6
Asset management.....	7
Human resources security	8
Job and person specifications	8
Staff awareness.....	9
Communications and Operations	9
Operational procedures and responsibilities	9
Systems planning and acceptance	10
Protection against malicious software.....	10
Back-up procedures	11
Network and infrastructure management.....	11
Media handling and sensitivity.....	12
Exchanges of information and software	12
Internet and e-mail	12
Physical and environmental security	12
Secure locations.....	12
Equipment security.....	13
General controls.....	13
Access control	14
Business requirement for access control	14
User access management.....	14
User responsibilities	14
Network access control	15
Operating system access control.....	15
Application access control	15
Monitoring system access and use.....	16
Mobile computing and remote users.....	16
Federated arrangements and external interfaces	17
Information systems acquisition, development and maintenance.....	17
Security requirements of Systems	17
Security in Applications Systems.....	18
Cryptographic controls.....	18
Security of systems files.....	18
Security in development and support processes.....	18
Information security incident management.....	19
Business continuity management.....	19
Aspects for business continuity management.....	19
Compliance.....	20
Compliance with legal requirements	20
Reviews of security policy and technical compliance.....	21
System audit considerations.....	21
Conclusion.....	22
Appendices	22
Acceptable hardened locations	22

Version Control

Version	Date	Author	Changes / Comments
0.1	25/08/2009	Ray Collins	Creation and populated
0.1	26/08/2009	Ray Collins	Updated and issued to Brian Durrant
0.2	05/01/2010	Various	Updated with changes and comments from CST
1.0	08/02/2010	Various	Document approved by Executive Board
1.1			Public version – sensitive information removed

This document and the attached Appendices recognize all trademarks, copyright and the IPR of their respective owners.

Introduction

The purpose of this document is to state the London Grid for Learning's overall information security policy.

The use of the 'shall' indicates a mandatory requirement. The use of the word 'will' indicates a desirable requirement.

This document is supported by a number of other supplementary documents to be found at www.policies.lgfl.net.

This document is restricted to the LGfL, its staff and direct suppliers.

Security policies - management direction

Purpose: To provide an overarching structure to the approach taken, and management direction given, to the subject of information security by the London Grid for Learning (LGfL).

The information security policy is driven by statutory requirements and non-statutory influences, such as good business practice.

The statutory requirements include:

- Children Act 2004 (et al)
- Data Protection Act 1998
- Computer Misuse Act 1990 / Police and Justice Act 2006 (Sections 35 – 38)
- Human Rights Act 1998

Which are supported by the following strands within the 'HMG Security Policy Framework':

- Security Policy No. 1: Governance, Risk Management and Compliance
- Security Policy No. 2: Protective Marking and Asset Control
- Security Policy No. 3: Personnel Security
- Security Policy No. 4: Information Security and Assurance
- Security Policy No. 5: Physical Security
- Security Policy No. 6: Counter-Terrorism
- Security Policy No. 7: Business Continuity

Whilst some of the strands within the HMG document may, at first glance, seem far removed from the LGfL's sphere of activity, further consideration of how much adverse impact could be obtained by a specific denial of service suggests all has relevance.

The intended audiences for this information security policy are:

- LGfL staff
- Clients and customers of the LGfL
- Suppliers to the LGfL

The security policies are binding on staff members and contractors employed by the LGfL.

The sections in this information security policy are based on the controls to be found within ISO 27002.

- Security policies - management direction
- Risk assessment and treatment
- Organisation / governance of information security
- Asset management
- Human resources security
- Communications and operations
- Physical and environmental security
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Each of these sections shall be supported by a policy document in its own right.

The current version of these documents is to be found at <http://policies.lgfl.net>

All information security areas shall be documented.

Each organisation that has dealings with the LGfL is expected to respect these policies and to have in place similar instruments. Where a new LGfL contract is let, or an existing contract renewed, these policies will be included in the contractual agreements.

Where a situation is not covered explicitly within the document set, the underlying values and processes should be used as if it had been.

Risk assessment and mitigation

Purpose: To articulate the approach taken to assessing hazards to information and the mitigation of risks

The LGfL has identified a Senior Information Risk Owner (SIRO). This person is responsible for identifying the risks, their assessment and how they will be addressed.

In order to achieve this, all information assets shall be owned by the identified Information Asset Owners (IAO).

The IAO is responsible for identifying the hazards to their assets, their risk assessment and how they will be mitigated.

The IAOs will work to the SIRO in producing a comprehensive set of risks, their assessments and mitigation steps which will be entered into the LGfL Risk Register.

The actual process for determining risk is described in the LGfL Risk Register Process document to be found at www.policies.lgfl.net.

Organisation / governance of information security

Purpose: To identify how information security will be managed and controlled.

Responsibility for the implementation and maintenance of the Information Security Policy lies with the LGfL Core Strategy Group (CST) headed by the LGfL CEO. The role of the Senior Risk Assessment Officer (SIRO) lies within the CST.

Each member of the CST carries an individual responsibility for ensuring that the supplier, for whom they are responsible as the key LGfL liaison officer, adheres to the information security policy. They are also responsible for ensuring all incident investigations are sanctioned and undertaken by competent staff in a legally defensible manner.

The information security policy shall form a standing item on the CST Agenda, and the CST will collectively review the policy on an annual basis.

All authors of information security documents shall ensure the documents have the following characteristics:

- Version numbering
- Dates of creation and amendments
- Protectively marking
- Destruction method stated

All authors of information security policy documents shall ensure they are aligned with the components of the ISO 27002 standard.

All organisations in the LGfL supply chain, including the LGfL, shall have an overall information security policy which covers the requirements of the Becta 2009 Information Handling Guidelines and the HMG Security Policy Framework.

Asset management

Purpose: To determine the manner in which assets will be managed

All assets, including information assets, of the LGfL shall be classified. The information assets shall be maintained in the LGfL Asset Register by the Senior Information Risk Officer (SIRO) as well as the designated member of staff responsible for implementing controls.

Information assets should be organised into asset sets and each set shall be owned by an Information Asset Owner.

The Information Asset Owners shall report to the SIRO for this function.

Information assets shall be individually and collectively classified to the following level of detail:

- Inclusion in which set of information assets
- Impact level – minimum to be allowed
- Likely protective marking requirement - advisory
- Purpose - allowed
- Disclosures – to whom
- Confidentiality, Integrity and / or its Availability

The documenting of stored attributes shall be to a consistent standard and shall be reviewed within the context of the emerging Federated Arrangements recommendations.

The Information Asset Owner shall be responsible for documenting the assets' requirements for:

- Classifications
- Degree of protection – encryption in storage and transmission
- Special handling
- Immediate actions on security breaches
- Auditing and incident handling
- Location
- Federated arrangements
- Inclusion in Privacy Statements

A programme of systematic intrusion testing shall be implemented to test the integrity of the assets.

The SIRO shall be responsible for ensuring compliance with the overall impact level / protective marking scheme for all assets.

The guidance and description of the mandatory procedures required for impact levels, protective marking and aggregation of data sets for Confidentiality, Integrity and Availability is given in a [separate information security policy document](#) to be found at www.policies.lgfl.net.

These include the standards requirement for the exporting / importing of data requiring impact level assessment for aggregation purposes.

All documents and screen displays containing personal information and commercially sensitive or confidential information shall be assessed in respect of its impact level and be appropriately protectively marked as shown in this table:

Impact Level (input)	Protective Marking (output)
0	NOT PROTECTIVELY MARKED
1	PROTECT
2	PROTECT
3	RESTRICTED
4	CONFIDENTIAL
5	SECRET
6	TOP SECRET

Human resources security

Job and person specifications

Purpose: To remove or mitigate the risks of human error, theft, fraud or misuse of facilities.

All employees shall be made aware of their responsibilities with regard to information security and are responsible for complying with the LGfL's Policies and Guidelines.

These responsibilities include both specific job-related responsibilities and those roles contained within the LGfL Information Security Policy. Access to specific information shall only be given where the person's role requires it.

Security responsibilities shall be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

Potential recruits shall be adequately screened, especially for sensitive jobs. All employees and third party users of information processing facilities shall sign a confidentiality (non-disclosure) agreement.

A statement on compliance with the CRB Code of Practice shall exist in all organisations.

All staff in the LGfL supply chain that have access to children or their personal data in clear (electronic and / or paper) shall be subject to Enhanced Criminal Record Bureau (CRB) checks.

CRB checks shall be undertaken on the relevant staff every two years.

The overall information security policy shall include statements on the child protection arrangements for personal information held at off-shore locations.

All organisations shall review their practice against policy in the area of CRB Disclosure on a regular basis.

Staff awareness

Purpose: To ensure that staff are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

The LGfL CST shall determine what is required to make staff aware of the need for information security, and make appropriate arrangements, including the production of Information Security Guidelines documentation. This shall include examples of security incidents.

Staff shall be trained in security procedures and the correct use of information processing facilities to minimise possible security risks.

Communications and Operations

Operational procedures and responsibilities

Purpose: To ensure the correct and secure operation of information processing facilities.

The LGfL Operations Manager, in consultation with other managers, is responsible for all operational matters on networks, systems, and supporting the technical aspects of applications.

Other LGfL personnel have responsibility for specific applications and their business-related delivery requirements.

These systems and applications are:

System / application	Personnel	Supplier
Office productivity	Office Manager	
Learning Platform	Learning Platforms Manager	Fronter
e-Admissions	Admissions Operations Mgr	Atomwide
Content	Content Manager	
Core locations	Operations Manager	Synetrix

These personnel shall identify their technical support requirements and liaise with the Operations Manager in marrying the business requirement with the technical requirement; in all instances the information security policy will determine the security levels to be employed.

Appropriate training shall be provided for all employees who operate information processing systems. No operation of systems will be allowed to persons who are not competent.

Systems planning and acceptance

Purpose: To minimise the risk of systems failures.

The LGfL has a roadmap for the development, enhancement and maintenance of systems. Appropriate programme and project management methodology shall be used for major new developments. This methodology shall include ensuring the operational requirements of new systems are established, documented, and tested prior to their acceptance and deployment.

Development shall take place on a separate development environment to that of the production system.

No system shall be deployed until the appropriate business manager and Operations Manager have signed off the User Acceptance Test outcomes.

Advance planning and preparation shall be undertaken on at least an annual basis to ensure the availability of adequate capacity and resources.

The Operations Manager shall, in consultation with all other LGfL managers and suppliers, produce projections of future capacity requirements to avoid the risk of systems overload.

Protection against malicious software

Purpose: To protect the integrity of software and information.

The description of the mandatory procedures required to protect the integrity of systems from malicious software is given in a [separate information security policy document](http://www.policies.lgfl.net) to be found at www.policies.lgfl.net.

In overview:

- All systems and applications, including personal devices, shall have explicit precautions in place to prevent and detect the introduction of malicious software.
- All employees and users shall be made explicitly aware of their responsibility for protecting systems and applications from viruses.
- Any breach shall be regarded as a disciplinary matter.

Back-up procedures

Purpose: To maintain the integrity and availability of information processing and communication services.

The description of the mandatory procedures required to maintain the integrity of data from its loss due to systems failure is given in a [separate confidential information security policy document](#) to be found at www.policies.lgfl.net.

In overview:

- All data held in systems and applications shall be backed up in a form that enables full or partial recovery (image and full / incremental)
- The back-up and recovery procedures shall be documented.
- The back-up and recovery processes shall be tested on a regular basis.
- The recovery media shall be tested for integrity on a regular basis.
- The recovery media shall be held in a secure location at least 1 mile from the production site.

Network and infrastructure management

Purpose: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

The Operations Manager is responsible for the security of the network infrastructure.

No connection of any device shall be permitted unless expressly authorised by the Operations Manager.

All network equipment is located in secure areas and cabinets, with access restricted to authorised personnel.

Remote access to network equipment for management purposes shall only be via approved secure remote access technology.

All secure remote access shall be through 2-factor authentication.

The full range of infrastructure defences shall be deployed to at least the following depth:

- Firewalls
- Filtering
- Access control lists

No personal or confidential information shall traverse the core network unless it is sent by secure file transfer or is encrypted.

No personal or confidential information shall leave or enter the core network unless the session is digitally signed.

Further details on secure remote access, encryption and digital signing are given in a separate document to be found at www.policies.lgfl.net.

Media handling and sensitivity

Purpose: To prevent damage to assets and interruptions to business activities.

Personal data shall not be held on any personal device unless encrypted to FIPS 140-2.

No personal or commercially sensitive data shall be held 'in clear' outside of hardened locations.

These locations deemed suitable for the LGfL are listed as an appendix to this document.

Exchanges of information and software

Purpose: To prevent loss, modification, or misuse of information exchanged between organisations.

All personal information shall only be passed through a secure file transfer mechanism which meets the LGfL criteria.

Internet and e-mail

Purpose: To ensure correct use and avoid abuse of LGfL information systems.

All communications via the Internet and use of email must comply with the LGfL Internet and Email Policies to be found at www.policies.lgfl.net

Where possible, the end-user's name and location shall be anonymised where it is published or available e.g. in the e-mail address.

Physical and environmental security

Secure locations

Purpose: To prevent unauthorised access, damage and interference to business premises and information.

The locations listed at Appendix A are the only locations regarded as secure enough for the storage of personal and confidential information in unencrypted format.

At these locations critical or sensitive business information processing facilities shall be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.

They should be physically protected from unauthorised access, damage, and interference.
Utility service supplies shall be redundant and give high-availability.
The environment shall be controlled and fire-risk protected.

In all other locations, the environment shall be as close to the above as is possible with the minimum specification being:

All computer rooms, network racks, and media rooms shall be regarded as secure areas and shall be kept physically secure through the use of appropriate locks and other security measures.

Access by staff to any location will be by prior management approval and entry / exit shall be logged.

The protection provided should be commensurate with the identified risks.

All machine areas and operations rooms' personnel workstations shall operate a clear desk and clear screen policy to reduce the risk of unauthorised access or damage to papers, media and information processing facilities.

Equipment security

Purpose: To prevent loss, damage or compromise of assets and interruption to business activities.

The equipment in all machine rooms shall be kept at the correct temperature and humidity by the use of air conditioning systems.

The equipment shall be protected from fire by appropriate extinguishing gas fire protection systems.

The power-supply to all machines shall be protected by UPS systems, in turn protected with an off-Grid generator.

Users of computers or any related hand-held device shall be required to protect their own computer or handheld device from loss or damage and to take appropriate measures to keep information secure. In addition, before any computer or device is disposed of, steps shall be taken to erase all data stored internally to the standard set by CESG.

Equipment shall be physically protected from security threats and environmental hazards.

Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorised access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

General controls

Purpose: To prevent compromise or theft of information and information processing facilities.

Only authorised people are allowed access to areas containing sensitive information systems.

It is the responsibility of individual members of staff to keep their offices and personal computer secure.

Access control

Business requirement for access control

Purpose: To control access to information.

All employees shall have an individual access account. Shared accounts are not permitted.

The rights of each employee's account to access systems and applications shall be determined by their role.

The role's access levels are determined by the CST.

The employee's account shall be disabled when they leave employment and deleted within 6 months.

User access management

Purpose: To prevent unauthorised access to information systems.

Formal procedures shall be employed to control the allocation of access rights to information systems and services. These procedures are described in detail in a [separate information security policy document](#) to found at www.policies.lgfl.net.

In overview:

- The procedures shall include all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.
- Special attention shall be given to controlling the allocation of privileged access rights, especially those which allow users to override system controls.

User responsibilities

Purpose: To prevent unauthorised user access.

Users shall be advised through off and on-screen messages about the need to keep their access methods and codes confidential.

Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

The explicit acknowledgment of the user shall be recorded as it may be required for proof in any later proceedings.

Network access control

Purpose: Protection of networked services.

Access to both internal and external networked services shall be controlled.

This access control shall be of a sufficient level to prevent users who have access to networks and network services compromising the security of these network services by ensuring:

- Appropriate interfaces between the organisation's network and networks owned by other organisations, or public networks
- Appropriate authentication mechanisms for users and equipment.
- Control of user access to information services.

Operating system access control

Purpose: To prevent unauthorised computer access.

For each system and application, authentication shall be required of all users.

The level of authentication shall be determined by the sensitivity of the system and data stored within it. Access to Impact Level 3 and above shall be via 2-factor authentication.

Each system shall have an explicit policy for access, including password history and strong password restrictions.

Security facilities at the operating system level shall be used to restrict access to computer resources. These facilities shall be capable of the following:

- Identifying and verifying the identity, and if necessary the terminal or location of each authorised user
- Recording successful and failed system accesses.
- Providing appropriate means for authentication; if a password management system is used, it shall ensure strong passwords
- Restrict the connection times, and locations, of users.

Application access control

Purpose: To prevent unauthorised access to information held in information systems.

Shared network access to other user files and folders on local disks, folders within other email account and data held in other applications shall only be permitted by the application manager.

Users permitted to do so shall set up such shares ensuring that correct user names are used and any default public access shall be removed.

Logical access to software and information shall be restricted to authorised users. Application systems shall:

- Control user access to information and application system functions, in accordance with the defined business access control policy.
- Provide protection from unauthorised access for any utility and operating system software that is capable of overriding system or application controls
- Not compromise the security of other systems with which information resources are shared, be able to provide access to information to the owner only, other nominated authorised individuals, or defined groups of users.

Monitoring system access and use

Purpose: To detect unauthorised activities.

All systems shall record attempts at unauthorised access in log files.

These audit logs shall be checked on a regular basis by the operations staff and reported to the Operations Manager.

Systems shall be monitored to detect deviation from access control policy and record events to provide evidence in case of security incidents.

Mobile computing and remote users

Purpose: To ensure information security when using mobile computing and VPN facilities.

LGfL users shall use the secure remote access service which requires 2-factor authentication.

All remote devices shall be encrypted to FIP 140-2 where personal information is retained or processed on it.

Mobile and remote users shall take personal responsibility for the security of information on their computer. In particular users should:

- Regularly use a network connection to copy important information to the central CMS drive, or alternatively copy this information to an external data storage device.
- Update anti-virus software regularly.
- Take reasonable measures to ensure the physical security of their computer.
- Take measures to safeguard sensitive information from unauthorised access.

The protection required shall be commensurate with the impact level associated with the information being processed.

Federated arrangements and external interfaces

Purpose: To ensure a trust environment exists whereby information and access is controlled to at least the level required by the LGfL.

Each organisation engaged in the federated arrangement shall have a nominated member of their staff responsible for the identity management and federated arrangements compliance. This shall be the SIRO of each organisation.

A statement on the requirement and circumstances for identity management and federated arrangements shall exist in all organisations, as well as more explicit procedures and controls.

The LGfL shall review the existing LGFLaai Federation documentation, processes and procedures, and implement these across the supplier chain.

The security arrangements for the disclosure of all personal information shall be reviewed and enhanced to meet the requirements of the DPA. This will be undertaken in conjunction with the appropriate Information Asset Owner(s).

The LGfL shall undertake a compliancy audit of its supplier chain one year from the date of the acceptance of this set of recommendations.

All new organisations entering into a supply chain arrangement with the LGfL shall be compliant with the LGFLaai Federation requirements.

SIF shall not be used to pass information rated at IL3 or above.

Information systems acquisition, development and maintenance

Security requirements of Systems

Purpose: To ensure that security is built into information systems.

New developments and the enhancement of existing systems shall address security within the design process. The programme or project manager is responsible for ensuring the project documents design security into the system, and reporting these to the Programme / Project Board.

The security design shall include the infrastructure, business applications, and user-developed applications. The design and implementation of the business process supporting the application or service shall be considered for their security requirements.

Security requirements shall be identified and signed-off prior to the development of information systems.

All security requirements, including the need for roll-back arrangements, shall be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

Security in Applications Systems

Purpose: to prevent loss, modification or misuse of user data in application systems.

Appropriate controls and audit trails or activity logs shall be designed into application systems, including user written applications. These shall include the validation of input data, internal processing, and output data.

Additional controls shall be required for systems that process, or have an impact on, sensitive, valuable, or critical organisational assets. Such controls shall be determined on the basis of security requirements and risk assessments by the Information Asset Owner and the Senior Information Risk Officer.

Cryptographic controls

Purpose: To protect the confidentiality, authenticity or integrity of information.

Passwords shall be encrypted before transmission.

Cryptographic systems and, techniques shall be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

Security of systems files

Purpose: To ensure that IT projects and support activities are conducted in a secure manner.

Access to system files is restricted to authorised personnel responsible for managing and supporting the various servers.

In addition, development personnel responsible have access to systems areas on the development servers.

Security in development and support processes

Purpose: To maintain the security of application system software and information.

Changes control to any business systems shall be authorised by the LGfL manager identified above, who shall ensure that security is maintained.

Minor changes shall be logged on Software Change Control Log forms. Larger changes shall be detailed in a full software specification. Where a change is likely to cause a contract change request to occur, the LGfL CEO shall sign-off the request.

Managers responsible for application systems shall also be responsible for the security of the project or support environment. They shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

Information security incident management

Purpose: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

All users shall report any security incidents of which they become aware. Employees shall report incidents to the Senior Information Risk Officer.

The precise procedures are described in detail in a separate information security policy document to found at www.policies.lgfl.net

The SIRO is responsible for managing these incidents and reporting to the LGfL CST who will consider them, and organise appropriate dissemination to the supporting suppliers.

Individuals who commit security breaches shall be subject to disciplinary procedures.

Incidents affecting security shall be reported through appropriate management channels as promptly as possible.

All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organisational assets.

They shall be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organisation shall use the formal disciplinary process for dealing with employees who commit security breaches.

To be able to address incidents properly it is essential to collect evidence as soon as possible after the occurrence and to freeze the incident scene.

Business continuity management

Aspects for business continuity management

Purpose: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

The business of the LGfL is dependent upon all systems remaining operational.

The consequences of disasters, security failures and loss of service shall be analysed.

Contingency plans shall be developed and implemented to ensure that business processes can be restored within the time-scales stipulated in each contract. Such plans shall be maintained and practised to become an integral part of all other management processes.

Business continuity management shall include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Compliance

Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory, or contractual obligations and of any security requirements.

The LGfL's information security policy shall be maintained in line with relevant legislation. This legislation includes:

- Children Act 2004 (et al)
- Data Protection Act 1998
- Computer Misuse Act 1990 / Police and Justice Act 2006 (Sections 35 – 38)
- Human Rights Act 1998
- Employment Acts
- Freedom of Information Act
- Company
- Charity

All data processing activities shall be reviewed to ensure the data controller / processor delineation is correctly identified.

Processes and wording shall be produced to address the Privacy Statement¹ requirements caused through processing personal information about children and vulnerable persons. This shall include Subject Access Requests and Retention / Disposal arrangements.

Pro-active procedures shall be put in place to prevent Information Asset Owners processing data outside the notified Purposes.

The disclosure of personal information / attributes to other organisations shall be reviewed within the context of the emerging Federated Arrangement recommendations.

¹ Fair Processing Notice has been replaced by the term Privacy Statement / Notice

Reviews of security policy and technical compliance

Purpose: To ensure compliance of systems with organisational security policies and standards.

The requirement and circumstances for audit trails, along with incident handling and more explicit procedures and controls are described in detail in a [separate information security policy document](http://www.policies.lgfl.net) to found at www.policies.lgfl.net.

Each of the following LGfL groups shall meet to review information security policy and the implementation of these procedures.

- CST
- TSG
- MIG
- e-Safety Working Group
- Atomwide Liasion
- Synetrix PRM
- L2tICT

The security of information system shall be regularly reviewed. Such reviews shall be performed against the appropriate security policies and the technical platforms and information systems shall be audited for compliance with security implementation standards.

System audit considerations

Purpose: To maximise the effectiveness of and to minimise interference to / from the system audit process.

Appropriate audit tools shall be used on all servers and appropriate administrative applications, by authorised staff. These include the audit procedures within the internal office productivity files or event logs on all external systems.

There shall be controls to safeguard operational system and audit tools during system audits.

Protection shall also be implemented to safeguard the integrity and prevent misuse of audit tools.

The LGfL shall establish an 'end to end' audit trail for its services.

The LGfL shall establish explicit procedures for 'end to end' incident handling.

The LGfL shall standardise on 1 NTP, or establish the delta's between the 4 disparate NTPs.

The past and present uses of 'Sawmill' shall be reviewed to inform further usage.

A programme of systematic intrusion testing shall be implemented to test the integrity of the auditing.

Conclusion

This document provides the top level of the LGfL information security policy.

It will evolve, as will the supporting documents, as the organisations', LGfL and suppliers, maturity in this area also develop.

Appendices

Acceptable hardened locations

Location names removed from external circulation.

Name	Location