Birmingham City Council

Information Security Labelling and Handling Code of Practice

If you have inquiries about this Standard,
Contact the Information and Strategy Team on 0121 675 1431 or 0121 464 2877.

Standard Owner:	***Gerry McMullan – Information and Strategy Manager, Birmingham City Council***
Author:	***Mrs M A Westrop – Information Security Manager, Strategy Policy &Business Security Team Service Birmingham***
Version:	4.0
Date:	24/11/2011
Classification	NOT PROTECTIVELY MARKED

Produced in conjunction with SERVICE BIRMINGHAM

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose	Author
1.0	02/10/07	Approval by BTAG	C Hobbs
1.1	03/10/09	Changes for compliance with the GCSx Code of Connection BCC Response to Government Connection.	M Westrop
1.2	26/03/09	Changes suggested by ICF	M Westrop
1.3	08/04/09	Updates from review comments	C Hobbs/J Walker
1.4	15/04/09	Added classification and storage paragraph	C Hobbs
1.5	17/04/09	Amended storage paragraph	C Hobbs
2.0	22/04/09	Approved by BTAG	C Hobbs
2.1	09/07/10	Updated	M Westrop
3.0	01/09/10	Approved by BTAG	Caroline Hobbs
3.1	04/11/11	Review particularly incorporating new classification scheme and changes of defined term City or Council to council.	M Westrop
3.2	17/11/11	No comments received, no further changes required	Caroline Hobbs
4.0	24/11/11	Approved by BTCG	Caroline Hobbs

Document Distribution after approval

Version	Name	Organisation
All	All Staff	Birmingham City Council

Document Reviewers

Version	Date	Name	Organisation
1.2	08/04/09	CISG Members	Birmingham City Council & Service Birmingham
2.1	09/07/10	CISG Members	Birmingham City Council & Service Birmingham
3.1	04/11/11	CISG Members	Birmingham City Council & Service Birmingham

Document Approval by Birmingham City Council

Version	Date	Name
1.0	02/10/07	BTAG
2.0	22/04/09	BTAG
3.0	01/09/10	BTAG
4.0	24/11/11	BTCG

Overview

Authority[a]	Birmingham City Council – Head of Policy & Co-ordination
Owner[b]	Birmingham City Council – Business Policy Manager
Scope[c]	See introduction below
Review period[d]	This document should be reviewed at least annually or more often if there is change of circumstances.
Related Birmingham City Council documents	Information Security Classification Standard; Information Security Policy; Internet Use Policy; Internet Use Code of Practice; Access Control Standard; Disposal of Information Processing Equipment Standard; Information Sharing Protocol; Information Asset Management; Data Protection Policy; Authentication Security Framework; Records Management Policy; Password Control Standard; Flexible and Remote Access Code of Practice; Ten Email Security Principles for Elected Members; the 2008 Security Policy Framework and IA Standard Number 6 within the Manual of Protective Security; *Information Loss Standard* and the *Information Security Incident Response Standard.* Government Connect GSi Code of Connection for GCSx Version 4.1
BS ISO/IEC 27001:2005 BS 7799-2:2005 control references	Control Reference A.7 Asset Management A.7.1.1 Inventory of Assets A.7.1.3 Acceptable use of Assets A.7.2 Information Classification A.7.2.2 Information Labelling & Handling A.8.3.3 Removal of Access Rights A.9.1.1.Physical security perimeters A.9.2.1 Equipment siting and protection A.9.2.5 Security of Equipment off-premises A.9.2.6 Secure Disposal or Re-use of equipment A.9.2.7 Removal of Property A.10.1.3 Segregation of Duties A.10.8.1 Information exchange policies and procedures A.10.8.3 Physical media in transit A.11.1.1 Access control policy A.11.2.2 Privilege management A.11.3.2 Unattended user equipment A.11.3.3 Clear desk and clear screen policy A.15 Compliance with legal requirements A 15.1.1 Identification of applicable legislation A.15.1.3 Protection of organizational records.

[a] AUTHORITY: The person or organisation who is responsible for enforcing this Standard.
[b] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of this Standard
[c] SCOPE: The organisations or persons to whom the Standard applies.
[d] REVIEW PERIOD: How frequently the Standard should be reviewed.

2. PURPOSE OF THE LABELLING AND HANDLING CODE OF PRACTICE

The Birmingham City Council Labelling and Handling Code of Practice contain rules for everyone who handles information for the council, that is to say everyone within the scope of the *Birmingham City Council Labelling and Handling Standard*[e] and the Government Connect Secure Extranet (GCSx) Code of Connection requirements[f].

Those who are within the scope of the Standard must follow the advice in order to keep the council's information securely and comply with that Standard.

3. What is Processed Information?

Information or data is Processed whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: *it is difficult to say there is any activity directed towards the data, which does not amount to processing.*

4. CODE OF PRACTICE

Labelling and Handling Requirements for All Information

All information must be conspicuously labelled with its Security Classification[g].

Birmingham City Council managers are responsible for making sure all information is labelled with its Security Classification. Files must be marked with the highest security level that has been given to any item of information in that file. Information that is not specifically labelled will be considered to have a classification of "Not Protectively Marked".

Most information handled by the council is classified as "PROTECT" and is available only to a controlled number of people. More sensitive or valuable information might be classified as "RESTRICTED". Three categories are set out in the *Information Security Classification Standard* and readers should read this in conjunction with the Labelling and Handling advice.

[e] See the section on 'Scope' within the *Labelling and Handling Standard*.
[f] The Secure Government network GCSx: see the *Labelling and Handling Standard*.
[g] All Standards and Codes of Practice are available in PSPG database and on Inline.

ACQUISITION AND CREATION

When information is acquired or created, it must be given its Security Classification and handled appropriately for that Security Classification and additional particular requirements[h]. In every area of the council, it is the responsibility of all managers for that area to see to this.

Many particular requirements exist under the law, council standards and policies. For example, there are important requirements set out in the Data Protection Act; the *Birmingham City Council Internet Monitoring Standard* and the *Email Use Policy*. **Managers must make themselves and their teams familiar with all the particular requirements of their own business areas.**

Investigations have their own rules and evidential requirements. For more details about how evidence should be acquired, see the Investigation Access page in Inline[i] or contact Internal Audit.

STORAGE

All information used to conduct the council's business must be recorded in a filing system: this applies to all media, whether it is electronic, paper, photographs or other. All filing systems should have a

1. Security Classification based on the *Information Security Classification Standard*,
2. retention schedule and
3. data protection registration where personal data is contained in the database.

Managers are jointly and individually responsible for deciding and agreeing the Security Classifications and retention dates in their own business area[j]. Records Management Service[k] can help here.

Information must be stored appropriately for its Security Classification. For example, paper information classified as "PROTECT" or "RESTRICTED", should be locked away in cupboards. See the notes on physical security, below.

Storage of Information not owned by the Council

When anyone stores information on any council equipment[l], this must only be done in the course of authorised work for the council. For example, those who use the council's equipment may not store on any council computer drive copyrighted films or music which they have acquired for a purpose not connected with Birmingham City Council authorised work.

This restriction does not apply to information automatically stored by the system without the intervention of any user, as a result of permitted personal use of email or the Internet. The

[h] See the City Council's *Information Labelling and Handling Standard*

[i] Investigation access details are available on Inline, the City Council's intranet.

[j] Managers should follow the Council's Information Security Classification Standard and Retention Period Schedule

[k] 303 2498 at Nov 2010. Records management can carry out surveys to identify what records are held by a specific business area and can then produce retention schedules for the area concerned. Their service is, however, a limited one and some of it is chargeable.

[l] This includes personal and shared network drives and local hard drives

council reserves the right to monitor and investigate any information stored on its systems, including information stored as a result of personal use of email or the Internet. The council also reserves the right to discard any information stored on council equipment as a result of personal use of the council's systems.

When third party-owned personal information is stored on the council's equipment merely in order to facilitate the transfer information onto third party equipment, the party who provides that information will be responsible for its security unless there is an express provision otherwise. For example, if a home worker stores their private home email address on a council owned laptop, in order to send work home, the council is not responsible for the subsequent loss or misuse of that email address, except by express contractual provision.

Storage of information on Equipment not owned by the Council

When information owned by the council is stored on equipment not owned by the council, the information must still be handled in accordance with the council's policies, statutory duties and in compliance with any contractual provisions. For example, there are non-disclosure and access restrictions on information Processed by workers who work from home on their own equipment[m].

Storage of aggregated de-personalised data about ethnic origin, religion, criminality, etc.

Aggregated and de-personalised information, such as sensitive personal information about ethnic origin, must be stored separately from the personal information[n] to which it relates; but if the sample size is very small, it should not be stored at all because it can be traced to individuals.

[m] See the Flexible and Remote Access Standard

[n] Note that personal information is information linked to an identifiable living individual. It is "sensitive personal information" under the DPA if it is about racial or ethnic origins; political opinions; religious beliefs; trades union membership; physical or mental health; sexual life; commission of offences or involvement in legal proceedings for any offence. Sensitive personal information must have the security classification of RESTRICTED. The Data Protection Policy has stricter requirements for Sensitive Personal Data than for ordinary Personal Data. See the Council's Data Protection Policy.

ACCESS[o]

Access to council business information should be role-based and not individually-based[p]: this means that a person can access information classified as “RESTRICTED” or “PROTECT”, in the course of their work, only if their job or role within the council justifies this. Information should not be kept where only one individual can access it[q].

GCSx information

Everyone who accesses GCSx information must have security clearance and their identity should be checked, as stipulated in the GCSx code of connection[r].

No GCSx data should be accessed remotely but must always be accessed from Council-owned machines connected directly to Council-managed networks from equipment within Council premises. Therefore, **Blackberry connections to GCSx information are not permitted**.

Remote access

Information which is not connected to the GCSx network can sometimes be accessed remotely by permission, if conditions are met as set out in the *Flexible and Remote Access Standard.*

Mailbox labelling and handling

Emails are always classified as “PROTECT” or “RESTRICTED”, regardless of their content. See the council’s *Email Policy.*

Access to information Processed on systems - see also portable data below.

The council’s digital systems, information security policies, procedures and security arrangements are mostly intended to protect information contained in the computer systems. Much of the security is handled automatically by the system, but there will always remain vulnerabilities to various threats - viruses; hackers who invade wireless networks, etc. . Therefore always comply with the general security rules that protect the system, even when handling Not Protectively Marked (unclassified) information.

An individual responsible for the use of system data must always be identifiable in the system. Never reveal your password or share passwords and user identities; always log out of systems when the session is idle[s]. For example, if you access a case management system, you must enter the same user identity and password formalities, whether you are at a hospital site or somewhere else on the Birmingham City Council network.

[o] Please refer to the details in the City Council’s Access Control Standard.

[p] In line with ISO 27001:2005 A.10.1.3 & 11.1.1

[q] For details refer to the City Council’s Access Control Standard.

[r] Contact the ICF Business Policy Team for more information 675 1431 or 464 2877

[s] This advice is in line with ISO 27001:2005 A11.3.2

A note on Passwords and Password Protect Codes

The *Birmingham City Council Password Policy* and the Inline advice pages set out rules which include the important principle that **passwords should never be shared**.

Note that this applies to individual **passwords** you use when you log onto systems or equipment. There is a separate and unrelated Password Protect **Code**, which you can apply to documents separated from systems (email attachments; separately stored Microsoft Word or Excel documents, for example). These password protect codes must be shared so that, if one person is unavailable to open the file, others can do this. Passwords for password protected documents should be restricted to a list of authorized personnel, which is maintained within office procedures documentation, and which allows for passwords to be changed when necessary.

Access to non-system information - portable prints, copies and portable data generally[t] - three principles.

Portable information is contained in hard copy (paper, photographs, microfiche, maps etc) or on portable media (for example memory sticks, CD's, laptops, mobile telephones, Blackberries, palm held devices, cameras etc.). Access to portable information will not usually be audited or authenticated automatically, and therefore it is important to label, authorise, and maintain the audit trail.

1. Labelling

Portable information must be labelled with its security classification, and possibly with extra labels such as "personal" or "confidential". For example, investigation paperwork should be labelled RESTRICTED and should contain a note "If lost or stolen Return to Business Security [or Audit], Birmingham City Council." File names can be a useful place to put the label in electronic portable data, for example, a CD could contain a file named

```
"SecurityInvestigation123ABCRESTRICTEDdeleteApril2013"
```

Access must then be restricted appropriately: for example, extracts or details of audit investigations (classified as "RESTRICTED") should not appear on the lower classification Service Desk logs (classified "PROTECT").

2 Authorization and responsibility for portable information.

Copied information classified as "PROTECT" or "RESTRICTED", must always be the responsibility of a particular person. It is a manager's responsibility in each business area to decide what portable handling needs to be specifically authorized, and what is understood by a team as being generally allowed without the requirement for specific authorization. Managers must make sure this is clearly understood in their area of the business. Where there is no specific authorization required, labelling and handling responsibilities rest with the person who uses and transports the portable information.

[t] This advice is in line with ISO 27001:2005 A 10.8.1. See also the Remote Access Policy; the Flexible and Remote Access Standard; Flexible and Remote Access Code of Practice.

If “RESTRICTED” information is converted to any portable format and removed from the workplace for any reason, (for example, printed out and taken to an external meeting), there should be one person who agrees to take custody and responsibility for looking after it safely. If nobody takes responsibility by agreement, then the handler who printed it, is responsible. If you are handing “RESTRICTED” information to someone else who then becomes responsible for it, make them sign a receipt for it and keep the receipt as part of an audit log or you remain responsible.

See also the rules on transferring information and the single point of contact (“SPOC”) (Information transfer between organisations, below).

3. Audit log

All portable use of RESTRICTED information should be recorded in an audit log[u]. See also the notes on physical security below.

USE

Information must be used in compliance with council policy and statute and with the agreed Government GCSx Code of Connection. Of particular importance is the Data Protection Act, which contains rules about handling personal information.

Rules for the Physical security of information classified “PROTECT” or “RESTRICTED”.

1. When you discuss information classified “PROTECT”, “Confidential” or “RESTRICTED”, in public places, take care to keep the conversation from being overheard and take care what information is left on answering machines.
2. Copied information on memory devices such as memory sticks, CDs, telephones or iPods should only be downloaded onto processing equipment which is approved by Service Birmingham and meets minimum connection standards.
3. Information derived from systems with a GCSx connection should not be copied at all unless a business case has been made and approved by BCC management.
4. Portable information must be physically secured and must not be left unattended[v]. For example, do not leave it in a parked car; wherever possible hold and guard laptops and information storage devices personally; if you are the person responsible, store storage devices wherever you judge it is most secure. If information is lost or stolen, the person who is handling it at the time it was stolen must follow the *Information Loss Standard* and the *Information Security Incident Response Standard.*
5. You should take care to position your screen when viewing information classified “PROTECT”, “Confidential” or “RESTRICTED” on a computer, so that it is difficult for others to see, particularly if your workplace is accessible to the public. You should remove information promptly from view after use[w].
6. Do not leave prints and copies lying around. Collect copies from copiers and scanners immediately[x].
7. Rooms and cupboards containing information classified “PROTECT”, “Confidential” or “RESTRICTED”, and also processing equipment for such information, need to be locked.

[u] See the audit log template, available on PSPG database.
[v] This advice is in line with ISO 27001:2005 A.9.2.5
[w] This advice is in line with ISO 27001:2005 A.9.2.1
[x] Follow the City Council’s Disposal of Information Processing Equipment Standard.

Security perimeters should be protected by controlled entry gates, reception desks or locks[y]. All GCSx information on servers must be kept in dedicated secure rooms protected by locks and individual door fob devices must be allocated only to a controlled group of people authorized to access the GCSx information servers.

8. Unattended equipment must have appropriate protection – terminate active sessions when you leave your screen[z].

RETENTION

A retention schedule contains details about the different types of records held in a business area and how long they should be kept. Whenever possible, records should state the retention period in summary filing information. The Records Management Service have produced a Birmingham City Council Retention Schedule[aa].

BACKUP and ARCHIVING

All information held on the council's network is backed up regularly as part of an automated process. However information held on local drives, portable media and paper will need to be backed up locally[bb].

If information is no longer required for current business, but cannot be destroyed, it should be archived, either electronically or physically. Corporate systems are archived regularly but separate arrangements must be made for information held locally[cc].

Take care that information which is archived, or held as a backup copy, is given an appropriate Security Classification (see the *Information Security Classification Standard*). This may be the same as, or different from its original classification e.g. a document Not Protectively Marked when it is live, should be labelled PROTECT when is archived, to prevent multiple versions from being circulated. Conversely, some information, which was once RESTRICTED, may become Not Protectively Marked, because it ceased to be price-sensitive and thereafter forms part of a public record.

LOSS – THEFT OR ACCIDENTAL LOSS OR DISCLOSURE OF COUNCIL INFORMATION

If information is lost or stolen, the person who is handling it at the time it was stolen must follow the *Information Loss Standard*. It is management's responsibility (individually and jointly) to make all those who handle information carrying a protective marking of "RESTRICTED" aware of the consequences of the loss of such material. And it is management's responsibility to make everyone in their business area aware of what action to take in the event of any loss. All information security incidents must be reported to management swiftly.

[y] This advice is in line with ISO 27001:2005 A.9.1.1

[z] This advice is in line with ISO 27001:2005 A11.3.2

[aa] As at Nov 2011 telephone 303 2498.

[bb] For guidance on how to backup information, contact the Service Birmingham Service Desk on 464 4444.

[cc] For guidance on archiving, including retention schedules, contact the Records Management Service, as above.

DESTRUCTION

Information no longer required and of no archive value, must be destroyed. All information which is no longer required, and should be destroyed, is classified as RESTRICTED to stop its being inadvertently used. This is dealt with in three separate areas of policy[dd]:

> Removable Media
> The *Records Management Policy* details the rules for the disposal of paper and microfilm records, as well as removable storage devices such as memory sticks, CDs and floppy disks – but not telephones. See the Records Management pages on Inline for more information.
>
> Other media
> Where the digital information is stored on information processing equipment with integral storage, except for telephonic devices, (for example, laptops or personal computers), it should be destroyed as set out in the *Disposal of Information Processing Equipment Standard*.
>
> Mobile Telephones and Blackberries and palm held devices using the telephone network
> The Service Birmingham Telecommunications Team[ee] can advise you about current disposal procedures for these devices and any SIM cards they contain. This may involve data cleansing by an approved service provider.

TRANSFERRING INFORMATION CLASSIFIED AS "PROTECT" OR "RESTRICTED" INFORMATION[ff]

Before information is transferred, the sender must be satisfied that an appropriate individual has been identified to receive the information. The recipient must be made aware of any duty of confidentiality and other contractual obligations required by the Council when the information is sent[gg]. Always label transferred or copied information with the appropriate label, "PROTECT" or "RESTRICTED".

No GCSx data should be transferred across networks which are not owned or managed by the Council. Therefore, Blackberry transmission of GCSx data is not permitted.

Rules about email use can be found in the *Email Use Policy* and *Code of Practice*.

Electronic transfer of RESTRICTED information

"RESTRICTED" information should only be transferred if it can be confirmed that this is absolutely necessary. Transfer should be avoided if this is possible and the quantity of data transferred should be the minimum necessary.

[dd] note that destruction of information is part of the job of de-commissioning mobile devices or portable memory.
[ee] The Service Birmingham Telecommunications team should be contacted via the Service Desk (number above).
[ff] In line with ISO 27001:2005 A 10.8.3
[gg] In line with ISO27001:2005 A 10.8.1

Electronic transfer, of “RESTRICTED” information should always be done through **two level security**.

Two level security for information Processed remotely

RESTRICTED information should always be protected by authentication formalities. Whenever it is viewed remotely it should ideally be protected by an additional security barrier. The first security level is usually provided by the fact that to access the data, a data user (sending or receiving) must enter a password and user identity – as they would if the data was accessed locally rather than remotely. The second level of security is ideally achieved by the additional use of encryption.

For example, a Virtual Private Network connection can be set up so that a worker can view their computer terminal from home using internet connections to make their terminal at home appear as if it is the computer at work, At connection, the user will be required to enter a password, user identity and the data that travels to and from the home from Birmingham City Council will be encrypted. These safeguards – password and encryption - comprise the two levels of security necessary.

Additional security is also an option. Equipment or software which only allows access when the user passes another security barrier may be needed. The user might, for example, set up a Personal Identification Number code or have a security fob, which they use to unlock the software and hardware where they are processing the information. These measures should be weighed up, along with the costs and risks involved[hh].

World Wide Web File Transfers

There are specific rules about what you can, and cannot, transfer through a Birmingham City Council internet account: see the council’s *Internet Use Policy* and *Internet Use Code of Practice*.

If you transfer files through the world wide web and if, furthermore, this is not to an organisation connected to GCSx, you should ask the Service Desk to set up secure file transfer protocol (“SFTP”) through the City’s firewall.

RESTRICTED Information transfer – see also access to portable information, above.

Some RESTRICTED and sensitive personal information extracts may have to be carried around by council staff in order to carry out council business in remote locations. The business areas concerned should document the procedure and should consult Strategy, Policy and Business Security about what precautions are necessary. The user must develop formalities and logs[ii] to show when information is taken in and when it is returned or destroyed, and by whom. Documents not returned or destroyed must be periodically chased up and counted.

The person with custody of the information must additionally, take responsibility for information security lapses (see notes on portable information access, above). (If the transfer is between organisations, the SPOC will also be responsible).

[hh] If you want technical advice about this, contact the Service Birmingham Service Desk on 464 4444. This service may be chargeable.

[ii] See the template audit log on the PSPG database

For example, Sensitive RESTRICTED information for child protection may be needed by child protection courts. These extracts should be labelled, used and then returned or destroyed in a way approved by business security, and this process should be tracked in an audit log,

In general, before information is transferred to other organisations or individuals, the sender must be satisfied that this is an appropriate recipient and that they are made aware of any duty of confidentiality required by Birmingham City Council when they send this information.

The sender must also be satisfied that the recipient has the required security clearance whenever they transfer information Processed within the GCSx connection.

Information Transfer between organisations and SPOCs

Between different organisations, a single point of contact ("SPOC") should always be nominated and used by the information owner. The SPOC should have a coordinating role and oversight of operational activity with that particular third party[jj].   The SPOC must make his role well-known to all parties handling transferred information.

The SPOC has responsibility for the security of information transferred and the SPOC must make this fact known to all involved in the information transfer.

The SPOC is also responsible for the dissemination of security rules and controls for the transfer and the SPOC must manage communications between the two organisations about the data transfer.   The SPOC must have authority to raise the priority of security considerations above other operational convenience where necessary.

Third party access to information

Information should not be transferred or exchanged with other organisations unless there is a valid business reason for doing so. A council Single Point of Contact ("SPOC") with the third party should be the responsible for authorizing and controlling the transfer or exchange.

Agreements with third parties must bind them to return information and all copies and to keep it confidentially and to report any loss using the method stipulated in the *Information Loss Standard*.

When data is sent to third parties, personal details should as a rule be redacted or disguised. For example, software to test address label printing might be tested on a range of real data but the data could have a scrambled element to disguise the actual addresses on the database, but not change it so much that it loses its usefulness in the test exercise.

However, exceptionally the complete data, including personal or otherwise sensitive details, can be released in full by written permission of the Corporate Governance Team or a Director because the information itself is the subject of the investigation or other procedure and there is no other way to carry out the procedure but by use of the full original data.

[jj] Contact the ICF or BCC_Security@Servicebirmingham.co.uk for advice about identifying the SPOC

GUIDE TO VARIOUS METHODS OF INFORMATION TRANSFER: MAIL, FAX, &c for non-GCSx data

✗ = do not use this method ✓= permitted with precautions

Transmission Method	RESTRICTED	PROTECT	NOT PROTECTIVELY MARKED
By hand	✓ (with signed receipt for audit log)	✓	✓
By internal mail within the same building	✗	✓	✓
By standard post	✗	✓ Label the outside of the envelope “Confidential” if appropriate and make sure the envelope is opaque and not one with a window. There should always be a named individual recipient.	✓
By recorded/special delivery or courier[kk] Always use “tracking” services and arrange for parcels to be delivered with receipt signatures only.	✓ **Not recommended**. Note other guidelines for RESTRICTED or Confidential information. Label the outside of “To be opened only by the addressee” and log the transfer.	✓ Also note that there are Data Protection restrictions on sending personal information outside the country. Label the outside of the envelope “Confidential” if appropriate and make sure the envelope is opaque.	✓
By facsimile The recipient should be contacted to confirm they are on stand by and again to confirm they have received the communication. Label the cover sheet “Confidential” if appropriate.	NO ✗	✓ Note that there are Data Protection restrictions when personal data is sent abroad. The recipient should be contacted to confirm they are on stand-by and again to confirm they have received the communication.	
By email Label the subject header Confidential and/or RESTRICTED as appropriate.	✓ NB electronic transmission of RESTRICTED information needs two levels of security; always log the transfer for an audit trail.	✓ Note that there are Data Protection restrictions when personal data is sent abroad.	
By telephone	✓ Use equipment approved by Service Birmingham and do not use speakerphone and don’t leave information on answer phone. Information should be kept out of earshot of unauthorized personnel.		✓

[kk] There is no approved list of couriers. Use 'contracted suppliers' where there is already a corporate or local contract. Contact Corporate Procurement Services on 3-0303 to find out what contracts are already in place. If there is no existing contract, it is best practice to get three quotations and record why a particular firm is chosen.

GUIDE TO VARIOUS METHODS OF INFORMATION TRANSFER: MAIL, FAX, &c for GCSx data

✗ = do not use this method ✓= permitted with precautions

<table>
<tr><th>Transmission Method</th><th>RESTRICTED</th><th>PROTECT</th></tr>
<tr><td>Hard copies delivered by hand</td><td colspan="2">✓if all handlers (givers and receivers) are cleared to the appropriate level and storage is in locked cabinets in controlled areas.</td></tr>
<tr><td>By internal mail within the same building</td><td>✗</td><td>✗</td></tr>
<tr><td>By standard post</td><td>✗</td><td>✓ UK only by ordinary post. The envelope must be sealed and the word PROTECT must not be visible. The envelope must be addressed to a titled and named individual. A return address must be put on the envelope. Overseas post must be in the diplomatic bag.</td></tr>
<tr><td>By recorded/special delivery or courier
Always use “tracking” services and arrange for parcels to be delivered with receipt signatures only.</td><td>✗</td><td>✓ Within the UK only. The envelope must be sealed and the word PROTECT must not be visible. The envelope must be addressed to a titled and named individual. A return address must be put on the envelope.</td></tr>
<tr><td>By facsimile
.</td><td colspan="2">✗</td></tr>
<tr><td>By email
Always label the subject header RESTRICTED or PROTECT</td><td colspan="2">All e-mail sent to lower protectively marked GSi domains and the Internet MUST be routed via the central GSi mail relay using the organisation's GSi connection.
It is not permitted to forward GCSx email to any other system.
Encrypted files of GCSx information should not be emailed.
No GCSx data should be accessed remotely but must always be accessed from Council-owned machines connected directly to Council-managed networks from equipment within Council premises. Therefore, **Blackberry connections to any GCSx information are not permitted**.
Non GCSx material should not be sent to GSi through the GSi mail relay.</td></tr>
<tr><td>By telephone</td><td>✗
Strictly forbidden</td><td>✓ where the parties are sure of each others’ identities and of the conversation cannot be overheard.</td></tr>
</table>