POLICIES & PROCEDURES

TITLE	Data Protection & Security Policy
AUTHOR	REDBRIDGE INSTITUTE
RESPONSIBLE OFFICER	Resources Director
APPROVED BY GOVERNING BODY OR INTERNAL PROCEDURE APPROVED BY SLT	GOVERNING BODY
DRAFT DATE	
APPROVAL DATE	March 2015
REVIEW DATE	March 2018

Equality Impact Assessment

Completed by Redbridge Institute		**Not applicable – no significant changes**	√
Completed by London Borough of Redbridge		**Outstanding**	

INTRODUCTION

Redbridge Institute collects and processes information about all staff, learners and suppliers for administrative, academic, pastoral, health & safety and marketing reasons. It has a legal duty to protect that data and to ensure security of all systems.

DATA PROTECTION & SECURITY

Data Protection Act 1998 – 8 Principles

The Data Protection Act requires all organisations which handle personal information to comply with a number of important principles regarding privacy and disclosure. The Act states that anyone who processes personal information must comply with 8 principles. Data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

Registration with Information Commissioner

Redbridge Institute is registered with the Information Commission Registration Number Z5108400. Registration is renewed annually. Registration covers 8 purposes. These are publicly available on the Information Commissioner's Office website

Use of Data - Summary

- Operational purposes with regard to enrolment, education, examinations and monitoring
- Statistical purposes within the Institute and its funding bodies
- Sharing analysis with schools, colleges, funding bodies, local authorities
- Contacting prospective, current and past students for research, quality and marketing purposes
- Providing references for training or employment
- Providing financial data for credit purposes
- Health & Safety and Security reporting

Processing and Retention of Data

Staff and learner data is processed and kept electronically as well as in paper form. Credit card details are not processed or stored electronically other than processing of the payment through the standalone dial out terminal

Sharing of Data

Redbridge Institute may pass on information as follows:

- To funding bodies, examination and assessment boards, local authorities, central government, government agencies and other official organisations as required by statute and to Connexions and similar agencies for provision of ongoing advice and training and employment purposes
- To third parties acting as agents of Redbridge Institute – in the operation of Institute business only.

Information and Consent

Information about data processing is displayed on each form. Details of the Data Protection policy is sent to each enrolled learner and is displayed on the website and in our prospectus. Consent is obtained from all learners and staff for the processing of personal data.

Data Protection Procedures

1. Under the terms of the Data Protection Act 1998, the London Borough of Redbridge is the official Data Controller for data held at Redbridge Institute and has appointed a Data Protection Officer.
2. The Data Protection Officer at Redbridge Institute is the Resources Director
3. Members of the Senior Leadership Team will be aware of the detailed principles of the Act
4. All staff will be made aware of the basic principles of the Act at induction and will be responsible for following guidance given with regard to compliance
5. Before personal details are requested from any source (staff or general public), agreement must be sought from the Resources Director
6. All forms which will be used to collect personal details must be designed in accordance with standard Institute wording/layout and must be cleared by the Resources Director (see below)
7. The Resources Director will be responsible for notifying the Information Commissioner's Office of the purpose of each data collection process
8. Interviewing/Reception/Enrolment staff will be responsible for ensuring accuracy of information collected with regard to learner enrolment, for questioning doubtful data and for processing such information in a confidential manner before passing to MIS staff. Reception staff will then be responsible for blanking out credit card details on enrolment forms and for filing forms securely.
9. MIS staff will be responsible for processing personal student data promptly and in confidence and for ensuring secure storage of such information
10. IT staff will be responsible for ensuring compliance with relevant legislation in the use of IT systems, cookies and similar technologies.
11. Managers appointing staff will be responsible for ensuring staff are aware of the principles of the Act and of the procedures to be followed
12. Managers appointing staff will be responsible for ensuring accuracy of information collected and for processing such information in a confidential manner before passing to the Customer Service & Staffing Team Leader
13. The Customer Service & Staffing Team Leader will be responsible for processing personal staff data promptly and in confidence and for ensuring secure storage of such information

14. Where data is obtained from a source other than the data subject, the subject must be informed unless it is unreasonable to do so or there is a legal obligation which overrides the terms of this Act
15. Access to learner details will be restricted to administrative staff and educational management staff. No part-time tutor will be given access to individual learner details unless s/he directly teaches the individual concerned and such information is essential to the teaching process. In such circumstances, access will be restricted to essential information.
16. Access to staff details will be restricted to the Staffing Team, to members of the Senior Leadership Team and to individual line managers
17. The use of cookies and similar technologies will be controlled. Users will be notified as to use and consent sought where appropriate.
18. Learner details will be held in the Institute's MIS system which will be protected against unlawful access by the use of passwords and access levels. Details will also be held manually in files which will be stored in rooms which are not accessible to the general public. Such rooms will be kept locked (by key or key pad) at all times when no member of staff is present. Alarms will be used outside opening hours.
19. Credit card payment details will not be stored electronically. Paper credit card slips will be stored for banking reconciliation and audit purposes. These will be kept in a locked room and will not be stored with the individual's other data. The Institute will adhere to the Payment Card Industry Data Security Standard.
20. The recording, security and retention of CCTV images will be in line with the Institute's CCTV Policy and protocol
21. Data will not be transferred between sites unless there is an essential business reason for doing so.
22. If data is moved the person carrying the data will be responsible for ensuring that the data remains securely on his/her person at all times until safely handed over or securely filed elsewhere. If data is being transported via laptop or other electronic storage device or medium, it should be encrypted wherever possible and that equipment must remain with the individual carrying the data at all times. If transfer requires a period when the individual cannot keep sight of it at all times (for example overnight), the carrying device must be placed in a secure locked environment. Under no circumstances should any laptop, memory stick or similar device be left unattended or unsecured. The boot of a car is not a secure environment.
23. Guarantees will be obtained from any outside agency processing Institute data (after advice has been sought from Legal Services)
24. Security measures must be made clear when passing data to or from another service area within the Authority
25. All e-mails containing personal data should be deleted once processed
26. Regular mail shots to individuals should give the data subject the opportunity to check and amend information where appropriate
27. Disclosure of any information must be compatible with the notified purpose.
28. The Data Protection Officer must be consulted before any transfer of personal data to a country or territory outside the European Economic Area

29. Personal data will be kept no longer than is necessary for operational or legal purposes
30. When no longer required, all personal data will be cross-shredded internally or sent for disposal via a registered secure data disposal company.
31. Breaches of this policy may lead to disciplinary action which, under certain circumstances, could result in dismissal. Staff will be made aware that improper use of IT and credit card systems could result in either the user and/or the Institute or Council incurring civil or criminal liability.

IT SYSTEMS SECURITY

IT Systems Security is covered by the Institute's IT User Policy. The following key points apply:

- All systems, networks, hardware and software will be installed by or under the guidance of the IT Support Team
- Configuration and maintenance of routers, firewalls and other network security devices will be the responsibility of the IT Support Team
- No IT equipment may be connected to the Institute networks unless approval has been given by the IT Support Team
- IT equipment can only be moved with the authorisation of the IT Support Team.
- The IT Support Team will work with the Finance Team to maintain an inventory of hardware, software and licences. Regular stock checks will be undertaken.
- All hardware will be appropriately secured
- Access to rooms containing IT equipment will be by way of key or keypad. The learning resource room is an exception as this has public access.
- Servers will be protected by physical security & access control, fire detection, temperature & humidity control and by a stable electrical supply protected by UPS
- Protection against malicious software and hacking will provided by a multi-level approach involving Firewall, Router Configuration, Email Scanning and Virus Protection
- All workstations will have appropriate antivirus software installed which will be set up to update automatically
- Network traffic will be monitored for unusual activity
- The administrative network will be separate to the teaching/public network
- Servers will be backed up nightly
- All access to Institute systems will be by Login and Password.
- Password protocols must be adhered to
- Passwords must be kept secure and not disclosed to or used by anyone else
- Network accounts will be disabled on the last day of service or earlier in certain circumstances
- All IT equipment must be returned prior to last day of service
- All Users will be expected to comply with this Policy, the Code of Conduct and the IT User Policy, including email, internet and social media guidelines
- Any information stored on a computer may be subject to scrutiny by the Institute or the Council