heart of the south west
local enterprise partnership

Draft Information Security Policy & Procedures V 6 (JP/EJ)

Introduction

The Heart of the South West (HotSW) LEP is a strong and dynamic business-led partnership between the private sector, local authorities, universities and colleges. Our purpose is to lead and influence economic growth, job creation and prosperity across the Heart of the South West area covering Devon, Plymouth, Somerset and Torbay. As a partnership the LEP works with a wide range of organisations and individuals and this policy sets out the LEP's approach to information security and data management.

The policy is based on advice from the Information Governance Manager at Somerset County Council, the LEP's accountable body[1], and is held by the Council as one of its Departmental data policies. It is reviewed annually, or as required, by the Chief Executive and signed off at Board Level.

The policy covers the following areas, ensuring compliance with the relevant data protection legislation

1. Security & compliance of LEP IT Systems
2. Security & compliance of data related to LEP business
3. Disaster Planning Approach

Ultimate responsibility for information security rests with the Chief Executive of HotSW LEP, but on a day-to-day basis the Chief Operating Officer shall be responsible for managing and implementing the policy and related procedures.

The Chief Operating Officer will be responsible for audits of compliance every 6 months and ad-hoc as required.

1. Security & compliance of LEP IT Systems

a) HotSW LEP Staff

- HotSW LEP is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation is devolved to staff who may be held personally accountable for any breaches of information security for which they may be held responsible.
- Each member of staff shall be responsible for the operational security of the information systems they use. Failure to do so may result in disciplinary action.

[1] Note that for some investment programmes the LEP also uses Devon County Council as an accountable body. Somerset CC provide 'back office' services to the LEP

- Each system user shall comply with the security requirements that are currently in force in this policy, ensuring that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Agreements with external users from the LEP's Accountable Bodies and partners working with HotSW LEP in ways which require access to our information systems, shall ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

b) Access Controls to IT systems

HotSW LEP staff work remotely from home locations or hot desk at stakeholder/partners offices. Each member of staff has either a LEP laptop or tablet and a mobile phone which is their own responsibility to keep secure; this includes good practice such as keeping locked out of sight when in a vehicle or at home and taking appropriate precautions when travelling on public transport. All equipment is logged on an assets equipment register held with LEP Admin at Somerset County Council.

All software and hardware is setup and configured by the LEP's IT contractor (currently Bluegrass CS). HotSW LEP's internal network is Microsoft Office 365, with security principles set. Network access is available through hard wired and wireless connection, there is no public access to our systems, although team members do access public Wi-Fi.

NB: accessing public or guest Wi-Fi at partner offices needs to be risk assessed by asking how secure their networks are and considering this, versus the practicality of the team in needing to logon to be able to work effectively? SCC to advise

c) Laptops & Tablets

The LEP works with its IT contractor to review our systems to ensure the appropriate level of protection against cyber threats and breach of data.

LEP systems are accessed via 2 sets of passwords: -

a) An individual laptop login
b) An office 365 password which accesses emails, SharePoint, business skype etc. A password reminder is set every 3 months via safety certificates, request to login back into office 365.

In addition, LEP IT equipment is encrypted to protect against access to data on the hard drive in the event a laptop/or tablet is stolen or lost, this will then become the first level of securely logging onto laptops and tablets. *NB: currently subject of a quote from Bluegrass*

All staff are required to ensure that their screen's lock after 5 minutes of inactivity, so that a password is needed to log back in.

All passwords used at work must not be used outside of the business and never shared with any staff or public. To check complexity of password use https://howsecureismypassword.net

NB: To manage several passwords Bluegrass have suggested using www.lastpass.com and individual users can use last pass for free. There are paid for options, but you can start with the free version. The application runs from the web browser and does not need to be installed. There are browser extensions which are easily installed without IT support. Not investigated with the team yet.

All staff have individual, username and passwords to log onto their laptops and Microsoft Office 365 services. All passwords must be

- More than 8 characters long
- Include upper and lower -case letters
- Include a number
- Include a character

Antivirus software is as advised by the LEP's IT contractor and currently consists of the following. Bluegrass also actively monitor LEP IT for any issues.

- Fuse mail – Fuse mail provides business continuity services for email. It scans email and removes Spam and Virus threats but also ensures that during email outages the customer can continue to deliver email to you without disruption and that you can reply.

- ESET Endpoint protection – Anti Virus software also scans email and this is a duplicate process when cover is extended by Fuse Mail. However, Antivirus provides significantly more protection against threats which do not arrive via email.

HotSW LEP makes use of Office 365 cloud based services and all filing of documents is via SharePoint.

Bluegrass CS manage the LEP's Office 365 tenancy.

All staff are required to install the regular updates for MS Office and MS Windows notified to them on their laptops/tablets.

d) Back- ups

Bluegrass provide a continual automated backup of all the data held in SharePoint and Exchange (mailboxes) via Backupify.
Investigate with Bluegrass within quotation for disk and file encryption.

e) Mobile devices

Mobile devices such as smartphones and tablets require special security controls owing to the increased threat to data that working on the move presents.

All mobile devices owned by HotSW LEP staff, and used to access HotSW LEP information (such as public contacts in outlook, emails, calendar, files in SharePoint) are required to adhere to the following minimum controls.

- Protected from unauthorised access by at least a 6-digit PIN or a passphrase, or digit recognition (for iPhones)
- Configured to ensure they automatically lock after one minute of inactivity;
- Configured in such a way that they can be remotely wiped in the event of loss; (iPhones have an automatic facility called “find my phone” in order to do this and are able to be remotely wiped in case lost or stolen – this has been instigated). *NB: 2 of the team have android phones and a similar facility is currently being investigated.*
- Only have trusted applications from reputable sources installed and antivirus installed if using an Android device
- Receive automatic software updates from the manufacturer and other 3rd parties; and
- Receive software updates for security patches within a reasonable timeframe.

Current advice is that mobile devices do not generally have anti- virus installed as the threat is still considered low but growing and with Email being scanned we can consider the threat is mitigated. At present the same best practices for internet use applied to a mobile phone will protect against most threats. This does need to be kept under review.

NB: The use of tethering one’s mobile phones to a laptops/tablet to access public Wi-Fi – needs to be risk assessed (raised earlier in this document).

f) Use of USB sticks
LEP Core team members on occasion have to use USB sticks which carry power-point presentations when presenting at events. These sticks are not encrypted. Recommendation is that all PowerPoint presentations are sent in advance.

On occasion external people use USB sticks for power-point presentations and fit these into our laptops – again recommend that all presentations are emailed in advance.

h) Incident reporting and management

All staff need to be aware and be constantly vigilant of cyber threats at all times. Every incident no matter how small must be reported to Bluegrass CS & to the Chief Operating Officer and logged in our Cyber incident report log
NB: incident report process to be finalised
Typical incidents include

- Loss of hardware
- Loss of personal mobile devices
- Click on suspicious link
- Suspicious email
- Virus threat

NB: SCC to advise policy on whether it is notifiable to the data commissioner

i) Personal use of work laptops/tablets
It is anticipated that most staff will use their work laptops/tablets and mobile phones from time to time for personal use for emails, internet browsing, banking, shopping etc. All staff must bear cyber threats in mind and be as vigilant in their personal browsing using company IT equipment as they would be using them in a work environment, by ensuring they do not click on suspicious emails or click on suspicious links and follow the above reporting mechanisms when using work apparatus.

j) Staff leaving
All staff accounts are removed by Bluegrass CS upon leaving the employment of HotSW LEP. Equipment is returned to LEP Admin (at Somerset County Council) or recycled for a new user (upon which Bluegrass CS will ensure all assets are reformatted) or if the equipment is no longer viable, Bluegrass CS will ensure that all data is erased and LEP Admin will arrange secure destruction of the equipment.

2. Security & compliance of data related to LEP business

a) Data Asset Review

The LEP has followed advice from SCC in developing its measures to comply with the latest data protection legislation, namely the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR). The section above also is part of the LEP's approach to these and covers equipment, this section sets out the handling of data.

. The following matrix was agreed to summarise the LEP's approach:

	GDPR	**PECR**
New data	Explanation that the LEP will hold their data and what will be done with it, as per the Article 13 guidelines within GDPR	
Existing data	Explanation that the LEP holds their data and what is done with it, as per the Article 13 guidelines	Opt-in/out to check they still want to receive communications from the LEP

Communications will be sent to the LEP's database based on the above categorisation to ensure compliance with GDPR and PECR.
For new data, consent is sought from the following communications:

- Sign up to E-newsletters through MailChimp
- Contact forms on the website
- Referrals from the telephone answering service (South Somerset District Council who operate this on the LEP's behalf) to the LEP and onwards to signposting to third parties i.e. Growth Hub. The contact page on the LEP Website will be updated to ref GDPR and PECR, plus reference the LEP's privacy statement (which is also in the process of being updated)
- Registration for download of documents
- Project Funding agreements including bank details – our Accountable bodies who handle this information will be Local Authority GDPR compliant.
- Eventbrite used to organise events/registration
- LinkedIn/ Twitter
- Applications/CVs for recruitment purposes

The LEP will only ever seek to keep the data necessary to enact our business and project activities. For example, we won't ask or store a date of birth for marketing datasets, nor do we sell data onto third parties.

Personal data (CV's/ Application forms/ Company registration forms, Board members personal phone numbers/addresses are all filed in the cloud

b) Data Classification

Data is classified as below:

	Description	Stored	Examples
Personal Data	**Personal data** means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.	Office 365 outlook	Board Directors Name, address, Telephone, Email + home address for some. Stakeholders, Local Authorities, businesses
		Cloud filing	Board Directors - Birthdate & home addresses (company director registration forms)
		CRM	All above
Sensitive data	**Sensitive personal data** means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs or other beliefs of a similar nature, (d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) their physical or mental health or condition,	Cloud filing	Race/ ethnic origin & religious beliefs, sexual orientation YES for recruitment purposes + includes equality & diversity statements – which only need to keep for 12 mths then deleted Also, CV's + application forms of employees in our cloud filing.

	(f) their sexual life, (g) the commission or alleged commission by them of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.		Our accountable body Somerset County Council holds employee bank details for employee payroll
Confidential	Confidential business information refers to information whose disclosure may harm the business. Such information may include trade secrets, sales and marketing plans, new product plans, notes associated with patentable inventions, customer and supplier information, financial data, and more	Cloud filing	Programme Mgt via Mel Sealey for projects inc bus. cases, due diligence, bank details, funding agreements are filed in the cloud and are Devon County Council GDPR compliant. Accounts/budgets filed in the cloud ESIF Programme mgt filing – Sam Seddon at Somerset County Council.

c) File storage & Cloud use

HotSW LEP uses Cloud services for its own business use. Legislation requires the LEP notifies contacts and secures their consent where their data is stored outside the European Economic Area.

Work in progress.

File service	What's it used for	Transferred to third country	Risk Summary
SharePoint	General file storage		General file storage – backed up to Backupify (Datto backup solution, https://sso.backupify.com/sla)

	Backed up to the Cloud by Bluegrass CS		*NB: Bluegrass have risk-assessed their own SharePoint; Heart of SW LEP will need to do their own assessment of cloud computing which will be picked up in the Cyber Essentials certificate.* US Based service with EU privacy shield
Office 365	Email service		EU based service O365 is ISO 27001 certified Email service backed up to Backupify (Datto backup solution, https://sso.backupify.com/sla)
CRM will be web based	Business contact information including stakeholders, partner, directors' information No project information will be kept on CRM	Quotations sought and currently evaluating bid with a view to putting in place a CRM system to aid our GDPR compliance	To be confirmed once CRM chosen.
Vuelio CRM	External database used by our LEP Comms Manager to access media contacts		The media CRM is compliant from their perspective, however "opt-out" was not compliant to the new regs, but this may only apply to personal information, which doesn't include media outfits in the public domain.
Mailchimp	MailChimp is the world's largest marketing automation platform for email marketing software – used by COMM's Manager to send out HotSW LEP newsletters		Mail Chimp has annually certified its agreement to EU/US and Swiss Safe Harbor Frameworks since 2007. If located in the European Economic Area (EEA) or Switzerland or send to anyone in the EEA or Switzerland, then you must complete their data processing agreement. Under Mail Chimp's Terms of Use and Privacy Policy, each user

			promises that their use will be compliant with all applicable laws.

3. Disaster planning approach – *work currently still in progress*

The following process has been developed to guide the LEP's response in a range of scenarios

Risk level	What	Who's involved	Who needs to be notified?	COMM's templates in place	Timeframe for resolution
Risk level 1	1 network hacked	Bluegrass CS LEP CEO LEP Data Controller	LEP Chairman LEP COMM's Mgr LEP Mgt team LEP Board All affected Clients- who are the clients?	Email: problem and resolution Phone call template: problem, resolution and timescales Daily update phone call:	*TBC currently in progress and will be assessed within Cyber Security Essentials certification and our IT contractor*
Risk level 2	Full web server down Loss of data – client HotSW LEP Ransomware attack	Bluegrass CS – web/domain issues and rebuild LEP Data Controller LEP Core Team	LEP CEO LEP COMM's Mgr LEP Board All affected clients	Email: problem and resolution Phone call template: problem, resolution and timescales Daily update phone call: Board report: issue, resolution and financial risks/investment Follow up letter to clients: issue, resolution, future prevention	Ditto Ditto
Risk level 4	Loss of any client's sensitive data Full loss of a client's data Client	Bluegrass CS – web/domain issues and rebuild LEP Data Controller LEP Core Team	LEP CEO LEP COMM's Mgr LEP Board All affected clients	Email: problem and resolution Phone call template: problem, resolution and timescales Letter to all clients: issue resolution, action for clients	Ditto

	ransomware attack Loss of HotSW LEP sensitive data			Daily update phone call: Board report: financial implications, financial investments, risk of client loss, risk mitigation Follow up letter to clients: issue, resolution, future prevention Press release: issue, resolution and prevention measures Media response: LEP CEO LEP COMM's Mgr LEP Chairman LEP Board LEP Mgt Team LEP Core Team	

Data breach notification and response plan

As soon as a theft, data breach or exposure containing HotSW LEP Personal data or Sensitive data is identified, the process of removing all access to that resource will begin.

Topic	What will happen	By when
1. Breach discovered/ reported	Breach is discovered. Timestamp breach. Assemble response team LEP CEO to chair group LEP Data Controller LEP COMM's Mgr Tech team: Bluegrass CS	*TBC currently in progress and will be assessed within Cyber Security Essentials certification and our IT contractor.*
2. Investigation and remediation	All access to data is revoked immediately - who was it - What was taken - Is the information useable in the format stolen - What is the impact of the breach on the customer/client HotSW LEP to work with IT provider to	Ditto

	determine how the breach or exposure occurred, the types of data involved, the number of internal/external individuals and/or organizations impacted, and analyse the breach or exposure to determine the root cause. Further action from this point will be dependent on the status but could include the following: • Advise police or official organization, e.g. Information Commissioner, accountable body • LEP COMM's Mgr to advise and write communications • Notify LEP Board • External comms: media statement, update web page, e.g. regular updates, contact information and actions for affected clients • Review/ amend policy and practices	