Learners are co-funded by the European Social Fund

LIFT Community Grants Programme
Information Security Policy

Purpose

The LIFT Community Grants programme will ensure that its information assets are protected, and that at all times the information that it processes is secured in line with the LIFT Community Grants Programme 'Records Management Policy' and 'Norfolk County Council's Information Strategy'.

As the programme is being delivered by Norfolk County Council (NCC) as the lead deliverer, this policy is aligned with the overall NCC 'Information Security Policy'.

Information Security

Accurate, accessible information is essential in order for the LIFT Community Grants programme to carry out its work, but if that information is not kept securely it can become a liability.

Effective information security is essential to ensure:

- Information is kept safe
- Information is available when we need it
- Information is shared when it is right to do so
- We maintain our reputation and the trust of our customers
- We comply with the law and protect ourselves from legal action
- Personal information about staff and customers is kept private

Information security has three main strands:

Confidentiality	Information is protected from unauthorised access or disclosure
Integrity	Information is accurate and complete
Availability	Information is accessible to authorised users when required

Who this policy applies to

This policy applies to:

People

- All staff (including all permanent and temporary employees, agency and casual staff)
- Volunteers, students, interns and trainees doing placements with the County Council
- Third parties doing business with the County Council e.g. contractors and sub-contractors or acting jointly or in partnership with the County Council

Premises

- All premises used by the County Council for business or storage
- Anywhere that any of the people listed above work away from County Council premises

Systems

- The deployment and use of the County Council's electronic systems including all computers, peripheral equipment, software, memory devices, tablets, smartphones etc.
- All use of computer networks or other systems for sending information
- Security of hardware, software and information, and the security of assets that may be placed at risk by misuse of the information systems

Information

- All information, held in any format - electronic, paper, fax, microfiche, or any other format

Responsibilities

There are some officers with specific responsibilities:

Managing Director	Responsible for ensuring the County Council's compliance with legislation, regulation and guidance
Senior Information Risk Owner (SIRO)	The Executive Director of Finance is the County Council's SIRO Responsible (as delegated by the Managing Director) for ensuring effective systems and processes are in place to deliver the information security agenda Responsible for reporting any relevant information risk to the County Leadership Team
Caldicott Guardians for Children's Services and Adult Social Services information	Responsible for ensuring that the County Council handles service users' information in accordance with legal and ethical practice
Directors/Heads of Service	Information Asset Owners (IAOs) for the service Responsible for information held by the service

	Accountable to the Managing Director for ensuring the effective implementation of this policy in their service
Managers	Responsible for ensuring that the staff they manage have completed all necessary training, Responsible for ensuring that the staff they manage have read and understood all relevant policies and procedures and that they follow these procedures in carrying out their work
Information Compliance Group/BI and IM	Responsible for agreeing policies and procedures Responsible for the implementation and monitoring of policies and procedures
Information Compliance Manager	Responsible for assisting in monitoring compliance with this policy Responsible for advising staff on compliance with the procedures supporting this policy Responsible for assisting in the production of Privacy Impact Assessments Responsible for assisting in the drafting of agreements and contracts Responsible for maintaining a list of all the County Council's information sharing agreements for monitoring purposes
Departmental Records Management Coordinators	Pro-actively promote records management awareness and mentor and train departmental staff in records management Provide first line of support for Electronic Document and Records Management System (EDRMS) system Advise in design of retention policy and retention schedule Operational responsibility for physical records including secure destruction of electronic and physical records Assist in information audits Support implementation of new rules and acts Participate in records-management-related demand workstreams if required

Implementation

The LIFT Community Grants programme will implement this policy by following the implementation procedures listed at Appendix A.

Details of the policy will be made available to all staff and learners through the most effective means.

The policy will be available on the LIFT programme independent website which can be accessed by LIFT Community Grant Programme staff, Suffolk County Council the subcontractor, project staff and learners.

Suffolk County Council as the sole subcontractor will be made aware of the policy and where to access it, and will be required to sign the policy document, committing to its aims.

Review of Policy

This policy will be reviewed, and revised if necessary, at least once every eight months from the signing of the Community Grant Contract, or more often as necessary according to requirements.

Named Individual in charge of policy review and revision: LIFT Project Manager

Version No.	Published Date	Review Interval	Review Date Due	Actual Review Date	Reviewer Name	Approver Name	New Version No.	Comments
1	1/4/2019	8 Months	15 Dec 2019					

References

General Data Protection Regulation

European Union
European Social Fund
LIFT COMMUNITY GRANTS
LOCAL INVESTMENT IN LEARNING PATHS TO WORK
Norfolk County Council
Suffolk County Council
Learners are co-funded by the European Social Fund

Appendix A

Procedure	What it covers	Who it applies to
Clear Desk, Clear Screen Procedure	Ensuring information is not left unsecured in the workplace when not in use	CG Staff
Email and Electronic Diary Procedure	How to use and manage email and e-diary securely and effectively.	CG Staff
ID Cards and Building Security Procedure	How to keep buildings and contents secure	CG Staff
IT Equipment Security Procedure	Keeping IT equipment secure in and out of the office, taking equipment abroad, sharing it, and reporting it lost or stolen.	CG Staff
Skype for Business Procedure	How we manage information securely when using Skype for business	CG Staff
Working Away from the Office (Mobile and Flexible Working) Procedure	Managing the risks to the security of information when working mobile and flexible. Mobile and home working Inc. transporting information	CG Staff
Passwords and Network Security Procedure	Rules about managing passwords and other measures to ensure the security of NCC information.	CG Staff
Printing, Posting and Faxing Procedure	How to print, post and fax information securely	CG Staff
Online Surveys and Web Forms Procedure	Managing the risks of information held in online surveys or submitted by web forms	All CG staff using online surveys to collect information
Acceptable use of Facilities and ICT procedure	Ensuring facilities are used appropriately to ensure security of information.	CG Staff
Data Breaches and IT Security Incidents Management Procedure		
Data Breaches and IT Security Incidents Investigation Procedure		
Conducting Privacy Impact Assessments		