'Individual Growth, Individual People'

Head Teacher: Mrs M A Tyers

Newark Orchard School's Third Party Information Policy Requirements

May 2018

Administration Centre . Appleton Gate . Newark . Notts NG24 1JR . Tel : 01636 682255 . Fax : 01636 682266 . Email : tsoffice@newarkorchard.notts.sch.uk
London Road Site . London Road . Balderton . Newark . Notts NG24 3AL . Tel : 01636 682256 . Fax : 01636 682267 . Email : office@newarkorchard.notts.sch.uk
Web : www.newarkorchard.notts.sch.uk

Table of Contents

1. Introduction

1.1. Where information is processed by third parties on behalf of the Organisation, it retains responsibility to ensure that information is processed according to the law and to ensure efficient service delivery. To achieve this the following controls must be in place; managed by suppliers and monitored by our commissioners and contract managers.

1.2. These requirements are applicable to private sector companies under contract to deliver services to us and forms part of the contractual requirements.

1.3. Where a Supplier is engaged with us and a contract or support agreement predates and does not in our opinion cover these requirements, then upon approval, completion of the Compliance Agreement (Appendix E) will provide the necessary additional assurance.

2. Requirements

2.1. Information Security Incident Process

2.1.1. The Supplier must have processes in place to capture and manage incidents of breaching the policy requirements set out in this document. (See Appendix A for types of incident). This includes incident management plans which are tested and reviewed, and appropriate training to incident managers.

2.1.2. The Supplier must have processes in place which analyse trends in breaches which have occurred, and use this data to inform policy reviews, implementation of appropriate controls, targeted training and communications to employees.

2.1.3. Where regular performance reporting is required by us, the Supplier must provide security incident statistical data. Detailed incident management evidence must be supplied on demand.

2.1.4. The Supplier must notify all incidents to their Commissioner or Relationship Manager for formal notification to us as soon as they are identified and must update us on the investigation progress and final resolution as directed. Criminal incidents must be reported to law enforcement.

2.1.5. The supplier must meet the requirements of Appendix D (Incident Management).

2.2. Risk management

2.2.1. The supplier must enable and support risk management across the organisation. This includes meeting the requirements of Appendix D (Risk Management).

2.3. Information Governance and IT Security Training

2.3.1. The Supplier must ensure that its employees who process our data are aware of these policy requirements and any additional agreed procedures.

2.3.2. The Supplier must ensure that its employees receive:

2.3.1.1. An appropriate level of training before they process our data (e.g. induction training which includes relevant Information Governance guidance).

2.3.1.2. A level of training appropriate to their roles and responsibilities

2.3.1.3. Refresher training at an appropriate frequency during the course of their employment, but at least annually.

2.4. Home and Mobile Working

2.4.1. The Supplier must assess the risks presented by this type of working and determine (and document) what their mobile working policy is. This includes meeting the requirements of Appendix D (Home and Mobile working.

2.5. Requests for Information

2.5.1. The Supplier must disclose to us any information it holds on behalf of the Organisation in response to a statutory request for information, audits, formal complaints and routine enquiries.

2.5.2. Provision of information and position statements to us regarding potential exemptions to rights of disclosure for statutory requests must be supported within the relevant timescales of the Freedom of Information Act (2000), the Environmental Information Regulations (2004) and the Data Protection Act (1998).

2.6. Privacy Management

2.6.1. The Organisation is the Data Controller and the Supplier is the Data Processor for any personal data managed by the Supplier on our behalf.

2.6.2. The Supplier must complete initial registration and an annual notification of personal data processed with the Information Commissioner's Office.

2.6.3. The Supplier must take appropriate steps to safeguard the privacy of our Service Users and only process personal data held on behalf of us within the conditions of consent or necessity agreed.

2.6.4. When collecting personal data from service users directly, we must approve the relevant Privacy Notice and the Supplier must comply with the Notice's conditions. The minimum necessary personal data must be processed, and all processing must be justified, necessary and comply with the Data Protection principles.

2.6.5. The Supplier must refer all directly-received requests for access or amendments to personal data held on our behalf for approval, unless there is an agreed process in place to manage this.

2.6.6. Where the supplier proposes to create a new or amend an existing system/ process affecting the processing of personal data, the proposal must be referred to us for Privacy Impact Assessment (PIA) and approval.

2.7. Physical Security

2.7.1. Use of Our Premises:

2.7.1.1. Where the Supplier's employees are based in or utilise our premises, the Supplier must ensure that employees comply with our physical security policy (see Appendix B).

2.7.1.2. The Supplier must comply with requests from us to supply monthly data of those employees who it approves to hold our ID Cards. Such data must be sufficient to identify individual employees to manage their card entitlement.

2.7.2. Use of other Premises:

2.7.2.1. The Supplier must ensure that premises (and dedicated areas where our data is stored within premises) are protected against unauthorised entry and theft of or damage to our data.

2.7.2.2. Access to building entry keys and keys which secure rooms or storage equipment must be controlled and possession recorded.

2.7.2.3. The Supplier must regularly change access codes and change relevant codes immediately when a member of staff leaves its employment.

2.8. Secure Handling of Information

2.8.1. Confidentiality

2.8.1.1. The Supplier must ensure that its employees maintain the confidentiality of all our data to which they have access.

2.8.1.2. The Supplier must not share our data with third parties unless with our explicit permission, unless subject to a Court Order or other valid legal

requirement to disclose, and having advised and consulted us regarding the request prior to disclosure.

2.8.2. Sub-Contracting of Services

2.8.2.1. Where we approve the sub-contracting of elements of service delivery to other parties, it is the Supplier's responsibility to ensure that these policy requirements are met in full by the other parties, and that we are made aware of all parties in the supply-chain processing our data.

2.8.2.2. Sub-contracting in the context of this document is where the main Supplier gives access to our data to another Supplier with which it has a contract or agreement. Where Personal Data is being processed in this way, all Data Processors must comply with the Data Protection Act.

2.8.3. Security Classification

2.8.3.1. We comply with the Government Security Classifications Policy (GSCP). All information processed by us falls within the category of 'OFFICIAL', with some data falling within the caveat 'OFFICIAL-SENSITIVE'.

2.8.3.2. Suppliers must comply with this classification scheme when processing information on our behalf (See Appendix C).

2.8.4. Disposal of Data

2.8.4.1. Where the Supplier has the Authority to dispose of our data in accordance with Retention Policy (see 2.8.2) or by virtue of any additional agreement, the data must be disposed of by methods appropriate to its security classification (see 2.6.1 and Appendix C).

2.8.4.2. Destruction processes must ensure that the data is kept secure from disclosure to unauthorised persons until and during destruction, and that the data cannot be reconstituted after the destruction process.

2.8.4.3. It is the Supplier's responsibility to ensure these standards of destruction are met by any third party engaged by the Supplier to destroy our data.

2.8.5. Equipment Security

2.8.5.1. Devices Accessing our Data (desktops, laptops, tablets, mobile phones etc.):

- Users must ensure that all security functions are enabled on portable equipment, such as pin codes and password access.
- Users must not access our data on devices that are not subject to the Supplier's technical security management, or where other appropriate controls agreed by us are in place.
- Devices must not be shared unless there is a facility for users to access data using their own account credentials known only to individual users.
- Equipment must be switched off or 'locked' after an appropriate period of inactivity and require a password to re-access.
- When stored in office space, laptops must be secured with lock devices or in lockable storage to prevent theft.
- When laptops are used in users' homes, they must be protected from use by any unauthorised persons (i.e. anyone other than the employee), and must be stored out of sight when not in use to prevent theft.
- When laptops are being transported they must not be left unattended, kept out of sight when not being used, and (where available) stored in secure transportation equipment such as a code-lock case.

- Employees must return devices to the Supplier when their employment ends or their role no longer entitles them to such equipment.
- Employees must not take devices abroad unless a) there is a strong business need approved by the Supplier's governance processes and by us, and b) there are sufficient security controls in place on the device to allow its use without exposing our data to malicious activity or unauthorised disclosure.
- Users must report lost or stolen equipment to the Supplier immediately and where any of our data is at risk the loss must be handled as a Security Incident (see 2.1).

2.8.6. Asset Management (Hardware)

2.8.6.1. A register must be maintained of the physical hardware items which the Supplier uses to access our data. Assets must be uniquely identified, have an identified custodian, and have up to date details of versions of security software installed.

2.8.6.2. The register must be promptly updated for new and decommissioned items, change of custodian and security software so that it remains current.

2.8.7. Removable Storage Media

2.8.7.1. Removable storage media refers to USB drives, CDs, DVDs, secure digital cards and devices which permit the storage of data on memory cards, but also refers to hard-copy such as paper files.

2.8.7.2. Where we have consented to the use of removable media, the Supplier must encrypt to an appropriate level any device storing our digital data that would cause damage or distress if it were lost or stolen.

2.8.7.3. Ensure that the level of security applied to office-located devices is applied to our data on removable media being used away from the office.

2.8.7.4. Personal data must only be held on removable digital media for transfer purposes and must be deleted once copied to its formal storage location.

2.8.7.5. Paper records must be stored in lockable equipment or dedicated rooms with access to keys or codes managed (see 2.5.2.2.). Such accommodation must include appropriate protection against fire and flood.

2.8.7.6. Paper filing systems must be well maintained, using clear, logical and consistent referencing and kept in good condition to support identification and retrieval.

2.8.7.7. When paper records are being transported they must not be left unattended, kept out of sight when not being used, and (where available) stored in secure transportation equipment such as a code-lock case, separate from our electronic equipment.

2.8.7.8. Where paper records contain our Official-Sensitive data, removing them from storage must be a logged activity, with manager approval or a managed process which authorises removal in clearly described circumstances.

2.8.7.9. Where paper records are in the custody of a third party storage provider, this is a sub-contracting arrangement and 2.6.2.1. above applies. The Supplier must ensure that detailed inventories are maintained to ensure the effective identification and retrieval of individual files and that storage and transfer processes offer appropriate levels of security to the security classification of the data.

2.8.7.10. The supplier must maintain a removable media policy for the storage of information that:

- Controls access to, and the use of removal media.

- Limits the type of media that can be used,
- Defines user permissions, and the information types that can be stored.
- Ensures that all clients and hosts automatically scan removable media for malware before first use, and any subsequent data transfer takes place.

Note: More technical control details can be found in Appendix D (Secure Configuration)

2.8.8. Acceptable Personal Use

2.8.8.1. Where information facilities (such as email) can be used to access our data, but can also be used for personal purposes, the Supplier must:
- Have a clear policy on what constitutes acceptable personal use, and
- Communicate this to employees .

2.8.8.2. Where such use is permitted, the Supplier must ensure that activity can be evidenced in the event of our data being misused in breach of 2.6.8.1.

2.9. Secure Use of Information Technology

2.9.1. Cyber-Essentials and the 10 Steps to Cyber Security

2.9.1.1. The Supplier must comply with the requirements of the UK Government's Cyber-essentials scheme. There are two levels of badges organisations can apply for: Cyber Essentials and Cyber Essentials Plus (includes external annual assessment). The sensitivity and criticality of information the supplier will process will dictate the badge we requires the supplier to have been awarded. The requirements of Cyber Essentials form the baseline security provision of the technology environment in which our data will be processed.

2.9.1.2. The supplier must comply with the requirements of the UK Governments "10 Steps To Cyber Security" publication. As well as containing similar technical controls to the Cyber Essentials scheme, it includes some important non-technical control requirements, such as Risk Management for example.

Appendix D contains a summary of controls found in Cyber Essentials and the "10 Steps To Cyber Security" publication. Please read this to find out what controls must be in place and adhered to.

2.9.2. Access Control / Managing User Privileges

2.9.2.1. The Supplier must restrict access to its IT network, and any systems where our data is held, to its authorised employees.

2.9.2.2. Each user must have their own username and password and credentials must never be shared.

2.9.2.3. Password strength must conform to the following standard:
- A minimum number of characters in length (e.g. eight characters);
- Differs from the associated username;
- Contains no more than two identical characters in a row;
- Is not a dictionary word;
- Includes a mixture of numeric and alpha characters;
- Has not been reused within a predetermined period of time (e.g. six months);
- Must not have been used for another account;

2.9.2.4. Employees must only have access to the information and user privileges they need to do their job.

2.9.2.5. Networks and systems must enforce regular password changes and limit the number of failed login attempts before denying access.

2.9.2.6. Where employees leave, or when they change to a role which no longer requires access or when access credentials have been compromised, the Supplier must:

- (Where we control access to systems) promptly inform our relevant Manager to allow accounts and permissions to be managed accordingly
- (Where the Supplier controls access to systems) take prompt action to ensure the accounts are managed accordingly.

2.9.2.7. The Supplier must limit the number of privileged accounts for roles such as system or database administrators.

2.9.2.8. Access by additional parties must be:

- For purposes approved by us
- Limited to fulfilling those purposes
- Time-limited
- Supported by commitments from those parties to safeguard our data
- Documented and auditable
- Closely monitored

2.9.2.9. The supplier must have the controls specified in Appendix D (Access Control / Managing User Privileges) in place and adhere to them

2.9.3. Monitoring

2.9.3.1. The supplier must establish a monitoring strategy and supporting policies. This includes having the controls specified in Appendix D (Monitoring) in place and adhering to them.

2.9.4. Malware

2.9.4.1. The supplier must ensure virus and malware protection is in place. This includes having the controls specified in Appendix D (Malware) in place and adhering to them.

2.9.5. Network Security (Including Boundary Firewalls & Internet Gateways)

2.9.5.1. The Supplier must ensure that all network devices are configured to the secure baseline build.

2.9.5.2. The Supplier must filter internet traffic so that only trusted traffic required to support its business is permitted .

2.9.5.3. Where the Supplier's employees are granted access to our IT network or systems, either through software which enables remote access or through the provision of an IT account, the Supplier must ensure that employees:

- Operate within an agreed scope of activity and our supervisory instruction
- Report any identified issues of concern to our supervisors
- Document the activities undertaken

2.9.5.4. The supplier must have the controls specified in Appendix D (Network Security (Including Boundary Firewalls & Internet Gateways)) in place and adhere to them.

2.9.6. Secure Configuration

2.9.6.1. The supplier must ensure that their systems are configured in the most secure way for the needs of the organisation. This includes having the controls specified in Appendix D (Secure Configuration) in place and adhering to them.

2.9.7. Patch Management

2.9.7.1. The supplier must ensure that the latest supported versions of applications are used and all the necessary patches supplied by the vendor have been applied. This includes having the controls specified in Appendix D (Patching) in place and adhering to them.

2.9.8. Email

2.9.8.1. The Supplier must ensure that employees are aware of the importance of correctly addressing emails (as with hard-copy mail), to reduce instances of loss of our data or it being received by an incorrect recipient.

2.9.8.2. Where the Supplier needs to send our Official-Sensitive data by email (or post), the Supplier must ensure that employees have been authorised to do so and follow the requirements under Appendix C. Where secure email facilities are not available (see 2.7.2), emails must be sent with our sensitive data in a password protected attachment, with the recipient informed of the password via an alternative method to email.

2.9.8.3. Where the Supplier's employees send our data to the incorrect recipient, the Supplier must manage this as a security incident and ensure the data is recovered. The Supplier must consult us if the data is personal in order to consider further actions as regards the data subject.

2.9.9. Secure Email

2.9.9.1. Where the Supplier has access to secure government systems such as PSN (GCSx), CJSM etc and the recipient is able to receive securely, then these facilities must always be used to send Official-Sensitive data.

2.9.9.2. Where the Supplier has access to accredited secure email tools (not falling within 2.7.2.1.) then these facilities must always be used to send Official-Sensitive data.

2.9.10. Federated Lync

2.9.10.1. Where the supplier has federated Lync functionality with us, the facility must not be used for the transfer of Official-Sensitive data and must not be the medium used to communicate and record contract decisions and actions.

2.9.10.2. The supplier must evidence appropriate policies and practices in its use of Lync in order for us to approve and maintain federation.

2.10. Information Management

2.10.1. Accessibility

2.10.1.1. The Supplier must ensure that our data held on its systems is maintained in such a way that those who have the rights to access can:

- Do so promptly;
- Easily identify and locate information
- Easily establish the most current and complete version
- Understand who they may share it with and under what circumstances
- Easily establish audit trails of services delivered and related authorisations, for use in our performance monitoring and internal or external auditing.

2.10.1.2. This must be achieved through:

- Clear internal ownership
- Security classification and marking (where required)
- Logical folder structures

- Titling conventions for folders and documents
- The use of metadata and standard classification schema
- The avoidance of duplication
- Ensuring all information is stored in shared systems, never with access limited to only one user.
- Clear sharing guidelines

2.10.2. Retention

2.10.2.1. Our data must be retained in line with our Retention Schedule and destroyed securely (see 2.6.2) with our explicit approval or by standing agreement with us which provides for the Supplier to destroy data once agreed criteria has been met.

2.10.2.2. Where the supplier destroys data, this activity must be evidenced by recording the criteria for destruction, approval, date and method of the destruction activity and certification of completion and follow the requirements at 2.6.4 above.

2.10.3. Asset Management (Data)

2.10.3.1. The Supplier must maintain a current and accurate knowledge of the data it holds in all formats, on what systems it resides and the physical locations in which those systems are stored.

2.10.3.2. Internal ownership must be established with owners aware of their responsibilities under these requirements.

2.10.4. Data Quality

2.10.4.1. The Supplier must provide quality data to support effective service delivery and decision making. Quality data has the following characteristics:

- **Accurate**: It must provide a true account of what it is intended to represent to enable informed decisions to be made. Limitations in the level of accuracy must be stated to help appropriate interpretation of resulting information. Maintaining the accuracy of Personal Data is a requirement of the Data Protection Act (see 2.4.5.).
- **Valid**: Data must appropriately reflect what it is intended to measure or report.
- **Reliable**: Data must be consistently calculated, recorded, analysed and reported over time in a way that provides a meaningful reflection of the situation to give managers and stakeholder confidence that progress towards targets reflects real changes rather than variations in data collection approaches.
- **Timely**: Data must be available frequently and captured promptly enough to be valuable.
- **Relevant**: Data must be defined/ selected, collected, recorded and analysed with the intended use and audience in mind so that it is fit for purpose and adds value.
- **Complete**: Data must be complete and comprehensive to ensure it provides a full picture of a current situation, and caveated where it is incomplete.

2.10.4.2. The Supplier must support regular reviews, sample auditing and provide commissioning feedback to achieve and maintain an acceptable standard of data quality.

2.10.5. Use of our Sharepoint Collaboration Sites

2.10.5.1. Where the Supplier is granted access to Sharepoint sites hosted by us which allow the sharing of and collaboration on information of mutual interest, the Supplier must ensure that:

- There is a register maintained of employees who have access to sites, and that the access is at all times necessary and therefore valid and available for auditing by us.
- Where employees leave the Supplier's organisation, or when they change to a role which no longer requires access or when access credentials have been compromised, the Supplier must inform the relevant Sharepoint Site Manager to allow accounts and permissions to be managed accordingly.
- Those with rights to add or edit documents must comply with the Site Owner's requirements over assigning document metadata, titling conventions and correct document library storage.
- Copies of documents containing our data available on the sites are not stored outside of the site or shared/ disclosed beyond the permissions group of the site without the permission of the Site Owner.
- Where a site is accessible by a number of Suppliers and Partners, any information which a Supplier does not wish to be available to anyone other than us and its own employees must be stored in a document library for the appropriate audience, provided by us.
- Its employees are aware that all information on the site is accessible to us and is information held by us for the purposes of the Freedom of Information Act (2000), with the Supplier offered the opportunity to present prejudice and public interest cases prior to disclosure.
- Where the Supplier is a Public Authority under Schedule 1 of the Freedom of Information Act (2000), its employees must be aware that disclosure of any data stored on a site in response to requests for information must be referred to us for clarification on whether the data is held for the purposes of the Act, and if so, for consideration of valid exemptions.

.

2.10.6. Usability

2.10.6.1. The Supplier must ensure that our data is held in formats that can be readily extracted from systems, retaining their integrity and usability by us.

2.10.6.2. The Supplier must therefore obtain our approval, before creating new (or amending existing) data systems, that data can be extracted in such a way that allows us to continue to utilise it with minimal disruption to services in the event of contract end or early termination.

3. Policy References

3.1. Compliance with these requirements is a requirement of the following policy:

- Our Sharing with Partners and Suppliers Policy

4. Breach Statement

4.1. Breaches of these policy requirements may result in contractual penalties in line with the provisions of the main contract between us and the Supplier. Serious breaches may result in withdrawal of access to our information and facilities, or exercising the contractual provisions for early termination.

Appendix A: Security Incident Types

The following is a list of security incident types which we require suppliers to have processes to identify, investigate, resolve, record and report.

Categories:	Description:	Incident Types:	Description:
3rd Parties	Breaches of Information Security Policy that affect or are caused by 3rd parties.	Gov Connect - GCSx	Issue with GCSx Connection
		VPN Misuse	Misuse of Support VPN
		Loss of Personal Information	3rd party loss of personal info
		Loss of Business Information	3rd party loss of business info
		Password Sharing	3rd parties sharing passwords
Breach of Policy	Breaches of Information Security Policy that are not reflected in one of the other options.	Email Misuse	Spam emails, abusive messages, improper use of mailing lists.
		Internet Misuse	Accessing sites in business time, inappropriate sites, use of un-authorised online systems
		Misuse of authority	Misuse of position, access or identity for personal gain.
		Personal Device	Adding an unauthorised personal device to the network or storing our information on a personal device.
		Information Handling	General lack of good information handling
		Insecure Password	Password for system does not match agreed standard.
		Staff Tailgating	Member of staff has tailgated in a building processing ourdata
		GCSx	Member of staff has abused the use of their GCSx account
Data Protection	Breaches of the Data Protection Act 1998 including loss, theft or disclosure of personal information.	Disclosure Personal Information	Confirmed disclosure of personal information to non-intended recipient.
		Loss of Personal Information	Loss of personal information with no certainty it has been disclosed.
		Theft of Personal Information	Theft of personal information with no certainty it has been disclosed.

Information Complaint	Complaints received from either the ICO or the public in relation to Information Handling Legislation.	ICO DP Complaint	Complaint from the ICO relating to non-compliance with the DP Act 1998.
		ICO FOI Complaint	Complaint from the ICO relating to non-compliance with the FOI Act 2000.
		Public FOI Complaint	Complaint from public relating to non-compliance with the FOI Act 2000.
		Public DP Complaint	Complaint from the Public relating to non-compliance with the DP Act 1998.
Lost/Stolen Equipment	Loss or theft of equipment (no O data stored).	Lost Equipment	Lost equipment (no Organisation personal data stored).
		Theft of Equipment	Theft of equipment (no Organisation personal data stored).
Network Security	Incidents that affect the Security of the IT Network storing Organisation data.	Spam Email	Spam emails received that pose a threat to the Network.
		Mailbox Size	Large mailbox size or large mailbox size increase within 24 hours.
		Systems Failure	Critical System offline.
		Virus Threat	Threat of virus to the network
		Folder Permissions	Reset or corruption of folder permissions for folders on the network
		Encryption – Laptop	Laptop discovered with no Encryption Software installed.
		Encryption – Desktop	Desktop discovered with no Encryption Software installed.
Password Sharing	Incidents where a password has been shared or used by another user.	Password Demanded	Employee has demanded password of a system from another member of staff.
		Password Shared	Member of staff has shared password of a system with another member of staff.
		Logged someone in	Member of staff has logged someone into a system under their own username without sharing the password.
Physical Security	Incidents where the physical security of a building or storage space processing our data is compromised.	Insecure Building	Building or storage facility discovered to be insecure.
		Public Unauthorised Access	Unauthorised person has been able to access a building or secured area.
Lost/Stolen Business	Incidents where our sensitive information has	Disclosure Business Information	Disclosure of our Sensitive Business information

Information	been lost, stolen or disclosed.	Loss Business Information	Loss of our Sensitive Business information with no confirmed disclosure.
		Theft Business Information	Theft of our Sensitive Business information with no confirmed disclosure.

Appendix B: ID Cards and Building Security Policy

1. Employees must not allow anyone to follow them through a security door (tailgating) without clearly displaying their ID Card.

2. Employees must carry their ID Card or Visitor pass and display it at all times when in our buildings, or to prove to a member of the public or staff of another organisation that they are representing us on official business. Otherwise, when outside of our premises they must keep their pass hidden to ensure personal security.

3. Employees must not share their ID Card with anyone, or share door codes or keys with unauthorised people.

4. If employees find a lost ID Card, they must hand it in to the nearest reception or security office.

5. If Employees lose their pass or it is stolen, they must report it to us.

6. All leavers must hand their pass to their line-manager as part of the leavers' process.

7. Employees must supervise all visitors that they allow into a secure work area at all times until they leave.

8. Employees must ensure door codes and security alarms are changed regularly. All employees must ensure offices are secure if they are the last person to leave at the end of the working day.

9. Senior leaders must perform regular checks of staff compliance with this policy.

10. All employees/ agency workers/ consultants/ elected members and Supplier/ Partner employees must assist senior leaders with checks of compliance with this policy.

11. Any ID Card which provides access to our buildings, or visibly identifies a person as being employed by us (or by an employer in partnership or under contract to us), or visibly identifies that a person has been approved by us to carry out a service, must be provided and recorded by us.

12. Any line manager or approver of requests on behalf of partner or supplier employees, must ensure that any access rights approved on staff application forms are valid.

13. The Information Governance Team must maintain a list of partners and suppliers who are approved to have our ID Cards.

Appendix C: Security Classification

Section 1: Classification

Definition:

All our information is classified as **OFFICIAL**. This includes:

- The day to day business of the authority and associated organisations, service delivery and public finances.
- Public safety, criminal justice and enforcement activities.
- Many aspects of security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

A limited subset of OFFICIAL information is called **OFFICIAL-SENSITIVE** and could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media:

- The most sensitive corporate information, such as organisational restructuring, negotiations and major security or business continuity issues
- Very sensitive personal information, such as information about vulnerable or at-risk people
- Commercially or market sensitive information
- Information about investigations and civil or criminal proceedings that could disrupt law enforcement or prejudice court cases

Baseline Security Outcomes:

- All official information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them

Marking:

- No Security Classification required for OFFICIAL information
- For OFFICIAL-SENSITIVE information you must mark it as OFFICIAL-SENSITIVE

- The marking must be placed in both Header and Footer of each document
- The font must be Arial, size 12, black.
- The same Security Classification must be used in the subject line of any emails sent via GCSX/ CJSM
- Where documents are saved into a network folder, the folder must be protectively marked at the highest level of the data within, e.g. OFFICIAL-SENSITIVE

- You must never change someone else's Security Classification without their express permission
- OFFICIAL-SENSITIVE might apply to just sections of a system or document so there is a need to ensure that we neither under protect or over protect information when designing systems.
- Access rights to IT systems must be limited to the minimum information needed, and usage of information monitored.

Section 2: Handling Guidelines

Official	Official (Sensitive)
Personnel Security	
• Appropriate recruitment checks • Mandatory training: Information Governance and Data Protection • Our Passes must be worn at all times • No tailgating permissible – be vigilant • You must comply with our guidance on secure passwords	• Appropriate recruitment checks (BPSS, or equivalent) • Additional training for handling protectively marked information • Access limited to 'need to know' and 'need to use'
Physical Security	
a) Document handling	
• Normal organisational controls • Clear desk • Clear screen – lock PC when away from desks • Compliance with Data Protection Act 1998 • Auto screen lock and system lock outs • Use agreed naming conventions for	**Physical** • Templates indicate official sensitive, descriptor and any additional handling e.g. retention, distribution • Tracking of physical assets (sign in/sign out, tracked delivery) • 'Need to know'/ 'need to use' access • Protectively mark information as OFFICIAL-SENSITIVE

documents • Ensure data is accurately recorded • Marking is not required for OFFICIAL documents • Ensure robust business continuity arrangements are in place • When sharing information ensure consent requirements have been considered • When sharing information ensure a privacy notice is in place	**Electronic** • Protectively mark information as OFFICIAL-SENSITIVE • Consider monitoring of activity • Marking of templates • Need to know/ use access • Consider encryption and additional access controls
b) Storage	
• Retain if unique (de-duplicate core records) • Standard building controls apply • Only save information to our provided/approved equipment • Save information to secure teamshare areas or systems	• Retain minimum required for purpose and enforce retention/ destruction controls • Limited access to storage e.g. consider locked locations, close monitoring of access (CCTV) access logs including denied access at personally identifiable level
c) Remote Working	
• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Protect equipment and information from use by unauthorised colleagues • Minimise local storage of information in physical or digital format	• Strong penetration testing • Consider multi-factor authentication requirements • Our owned equipment or portals which present data but limit or prevent local download or caching • Must have ability to lock away resources, secure filing and secure destruction facilities
d) Moving information assets by hand	
• Precautions against overlooking when working in transit • Abide by our policy and standards	• Authorisation for volumes of records, possible Privacy Impact Assessment requirement • Controls to prevent or authorise volume downloads • Electronic information must be sufficiently encrypted • Track movements
e) Moving information assets by post / courier	
• Check contents and destination • Use standard organisational mechanisms	• Include return address, never mark classification on envelope • Consider double envelope for sensitive assets

	• Consider using registered Royal Mail service or reputable commercial couriers' " track and trace" service
f) Moving information assets overseas (by hand or post)	
• Use accredited safe havens (NB: Safe Harbor is no longer a valid accreditation)	• Consider 'eyes on' or 'trusted hand' deliveries as part of a Privacy Impact Assessment • Use reputable and agreed couriers with track and trace and sufficiency of controls for the nature and volume of data
g) Bulk Transfers (Volume thresholds may vary)	
• Local management approval, subject to policy, appropriate risk assessment and movement plans • Appropriate contract clauses or Information Sharing Protocol	• Senior Information Risk Owner and potentially Caldicott Guardian authorisation required
INFORMATION SECURITY	
a) Electronic Information at Rest	
• Electronic Information will be protected at rest by default. This may be appropriate physical protection e.g. Foundation Grade data at rest encryption when physical control isn't guaranteed (such as on a laptop)	
b) Electronic Information in Transit	
• If protection is required, consider marking as Official Sensitive and sending via secure email • Consider providing access rather than transit • Non persona identifiable information may be emailed / shared unprotected to external partners / citizens, subject to local business policies and procedures	• Foundation grade encryption • Official secure networks (e.g. PSN) or other authorised network connectivity • Seek tracked access and ability for revocation of access • Seek limited timescales for access and ability to print or save (e.g. Digital Rights Management) • Access to be limited on the basis of both need to know and need to retain i.e. do they need the information locally or just access to view?
c) ICT Services	
• Cloud platforms might be possible dependent on a good understanding of the nature of data and residual risk to fall easily within the organisations risk appetite as assessed by Senior Information Risk Owner	• Cloud platforms are likely to require strong controls, assurance and audit • Use of cloud requires our specific SIRO approval of a detailed assessment

• End user devices will conform to the security principles defined in the End User Device (EUD) Strategy: Security Framework and Controls	
d) Removable Media (data bearing)	
• The use of removable media will be minimised, and other approved information exchange mechanisms must be used in preference • Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement • All portable equipment must be encrypted to protect the content, particularly where it is outside the Organisation's physical control	• Use of removable media may only be allowed if assessed by a Privacy Impact Assessment and specifically approved before use.
Telephony (mobile and landline), Video Conference and Fax	
• Follow organisational/ local guidance	• Details of sensitive material must be kept to a minimum • Recipients must be using Safe Haven fax procedures when faxing personal data and / or data marked with the OFFICIAL-SENSITIVE caveat • Validate the identity of participants
Disclosure (Statutory disclosures are separate from the classification scheme and require case-by-case assessment)	
• Much of the information in this domain is likely to be releasable under FOI or SAR unless an exemption is in force, or there is another statutory bar • Direct such requests for information to TransparencyTeam@essex.gov.uk • Other DPA requests, e.g., S10,s12,s14.s29 must be sent to InformationGovernanceTeam@essex.gov.uk • Where appropriate, non-sensitive information must be published for reuse	• Data and information will need specialist review prior to disclosure to ensure release is appropriate under legal and regulatory responsibilities

Disposal / Destruction	
• Remove duplication • Use organisational mechanisms or cross cut shredding as a minimum	• Dispose of with care using only mechanisms approved by us for disposal of confidential waste. • All data bearing equipment to be formally decommissioned by commercial disposal products where authorised by us to make reconstitution unlikely
Incident Reporting	
• Local reporting arrangements	• Escalation to SIRO, Functional Leader Teams and Internal Audit as appropriate for significant incidents • Report all information security incidents including near miss • External notification to ICO, GovCert / CINRAS, NHS may be required.

Appendix D: Cyber Essentials and 10 Steps to Cyber Security Controls

The following controls must be put in place and adhered to

1. **Network Security (including Boundary firewalls and internet gateways):**
   1.1. The supplier must ensure that:
   - Multi-layered boundary defences with firewalls and proxies are deployed between the untrusted external network and the trusted internal network.
   - Direct connections to external services are prevented and internal IP addresses are protected
   - Tools are used to monitor for intrusion and activity logs are audited on a regular basis
   - Penetration tests are undertaken on a regular basis, along with simulated cyber-attack exercises
   - Information, applications and computers within the organisation's internal networks are protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.
   - One or more firewalls (or equivalent network device) are installed on the boundary of the internal network
   - The firewall (or equivalent network device) administrative password is changed to an alternative, strong password.
   - Each rule that allows network traffic to pass through the firewall is subject to approval by an authorised individual and documented
   - Unapproved services or services that are typically vulnerable to attack are disabled (blocked) at the boundary firewall by default.
   - Firewall rules that are no longer required are removed or disabled in a timely manner
   - The administrative interface used to manage the boundary firewall(s) configuration is not be accessible from the internet.

   Note: The controls specified are taken from the Cyber Essentials scheme and the "10 Steps to Cyber Security" publication.

2. **Secure Configuration:**
   2.1. The supplier must:
   - Configure computers and network devices (including wireless access points) securely to reduce the level of inherent vulnerabilities, and provide only the services required to fulfil their role
   - Establish and maintain policies that set out the priority and timescales for applying updates and patches.
   - Create and maintain hardware and software inventories of every device and application used by the organisation
   - Lockdown operating systems and software, creating a baseline security build for workstations, servers, firewalls and routers
   - Regularly run automated vulnerability scanning tools against all networked devices and remedy any vulnerability within an agreed time frame

- Remove or disable any unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts)
- Change any default passwords for a user account to an alternative, strong password.
- Manage/control access to removable media including:
  - Implement policy to control the use of removable media for the import and export of information.
  - Limit the media types that can be used together with user and system access and the information types that can be stored on removable media.
  - All clients and hosts must automatically scan removable media: Any media brought into the organisation must be scanned for malware by a stand-alone scanner before any data transfer takes place.
- Remove or disable unnecessary software (including application, system utilities and network services)
- Disable the auto-run feature, to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed
- Enable a personal firewall (or equivalent) on desktop PCs and laptops, and configure it to disable (block) unapproved connections by default.

Note: The controls specified are taken from the Cyber Essentials scheme and the "10 Steps to Cyber Security" publication

3. **Access Control / Managing User Privileges:**

3.1. The supplier must establish an effective account management process that:

- Includes an account provisioning and approval process
- Limits user privileges
- Limits the number and use of privileged accounts, providing administrators with normal accounts for business use
- Monitors user activity, particularly access to sensitive information and the use of privileged accounts, and controls access to activity and audit logs
- Effectively manages and regularly reviews the requirement for all types of accounts, from creation and modification to eventual deletion, providing the minimum level of access required
- Ensures that each user must authenticate using a unique username and strong password before being granted access to applications, computers and network devices
- Ensures that accounts are configured to require a password change on a regular basis
- Ensures accounts are removed or disabled when no longer required

Note: The controls specified are taken from the Cyber Essentials scheme and the "10 Steps to Cyber Security" publication.

4. Malware Protection

4.1. The supplier must:

- Produce policies to manage the risks to the business processes from malware
- Establish anti malware defences across the organisation that are applicable and relevant to all business areas.

- Protect all host and client computers with antivirus solutions that will automatically scan for malware upon access
- Ensure that malware protection software (including program code and malware signature files) is kept up to date
- Regularly scan for malware across the organisation
- Prevent connections to malicious websites on the internet (e.g. by using website blacklisting).

Note: The controls specified are taken from the Cyber Essentials scheme and the "10 Steps to Cyber Security" publication

5. Patch Management

5.1. For all computers and network devices, the supplier must ensure that

- The software installed is licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.
- Software updates (including operating system software and firmware) are installed in a timely manner (e.g. within 30 days of release from vendors).
- Out-of-date software (i.e. software that is no longer supported) is removed, due to security patches no longer being available.
- Security patches are installed in a timely manner (e.g. within 14 days of release from vendors)

Note: The controls specified are taken from the Cyber Essentials scheme

6. Monitoring

6.1. The supplier must:

- Establish a monitoring strategy and produce supporting policies
- Implement an organisational monitoring strategy and policy based on an assessment of the risks.
- Continuously monitor all ICT systems and networks to identify unusual activity or trends that could indicate an attack.
- Analyse logs for unusual activity that could indicate an attack

Note: The controls specified are taken from "10 Steps to Cyber Security" publication.

7. Risk Management

7.1. The supplier must:

- Establish an effective governance structure that enables and supports risk management across the organisation
- Determine its risk appetite, communicating the level of risk it is prepared to tolerate.
- Have cyber risk as a regular agenda item in its Board meetings
- Record cyber risks in its corporate risk register to ensure senior ownership
- Produce an overarching corporate security policy together with an information risk management policy
- Structure policies and processes to support and enable a 'whole life process' for risk Management

Note: The controls specified are taken from "10 Steps to Cyber Security" publication.

8. User Education and Awareness

8.1. The supplier must:

- Produce and issue policies covering the acceptable and secure use of the organisation's systems.
- Ensure that its new users receive training on their personal security responsibilities
- Ensure that its users receive regular refresher training on the cyber risks to the organisation.
- Encourage relevant staff to develop and formally validate their Impact Analyses skills

Note: The controls specified are taken from "10 Steps to Cyber Security" publication

9. Home and Mobile Working

9.1. The supplier must:

- Create a mobile working policy that covers aspects such as information types, user credentials, devices, encryption and incident reporting.
- Educate users about the risks of mobile working / working from home, training them to use their mobile device securely by following the security procedures
- Ensure that all mobile devices are configured to an agreed secure baseline build.
- Ensure that data is protected both in transit and at rest.

Note: The controls specified are taken from "10 Steps to Cyber Security" publication

10. Incident Management

10.1. The supplier must:

- Ensure the organisations board takes the lead on the delivery of the incident management plans, and provides backing.
- Establish an incident response and disaster recovery capability, developing and maintaining incident management plans with clear roles and responsibilities.
- Regularly test incident management plans.
- Provide specialist training to the incident response team to ensure they have the skills and expertise to address the range of incidents that may occur.
- Report any criminal incidents to law enforcement

Note: The controls specified are taken from "10 Steps to Cyber Security" publication

Appendix E: Compliance Agreement

This agreement confirms that the Supplier has read our 'Information Policy Requirements for Suppliers' and commits to comply with the requirements for the duration of the contractual relationship and any further agreed period where the Supplier continues to process our data.

Supplier Name:	
ICO Registration Number:	
Signed by (on behalf of the supplier):	
Position:	
Date:	