Derbyshire Audit Services

Audit Guidance for Schools on the Procurement of IT Systems

Version History			
Version	**Date**	**Detail**	**Author**
1.0	October 2016	First Issue	Carl Hardman
1.1	January 2017	Suppliers update	Carl Hardman
1.2	May 2017	Suppliers update	Carl Hardman
1.3	July 2017	Suppliers update	Carl Hardman
1.4	December 2017	Supplier and data protection guidance update	Carl Hardman
1.5	July 2018	Suppliers update	Carl Hardman
1.6	February 2019	Suppliers update	Carl Hardman
1.7	June 2019	Suppliers update	Carl Hardman

Important Note

Inclusion within the Derbyshire Audit Services 'Audit Guidance for Schools on the Procurement of IT Systems' does not in any way constitute endorsement of any supplier or IT system. Neither the County Council nor its staff are responsible for making recommendations regarding the suitability of IT systems for use within schools or whether they will deliver the perceived benefits. Such evaluations must be made by school management and Governors in accordance with the school's financial procedures and legal obligations.

Background

All schools rely on a variety of IT systems and solutions to provide a range of services and educational support to teachers, governors, administrative staff and pupils. The range of IT solutions continues to evolve with the objective of improving the efficiency, management and reporting of key functions within the School. To facilitate the operation of such IT systems, staff and pupils' personal and financial data are frequently required to enable on-line payments, pupil performance monitoring and statutory reports to be produced. It is therefore important that, when assessing a new IT system, consideration is given to the School's Financial Regulations, current procurement law and obligations under the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR).

Dependent upon the nature of the IT system in use, personal or financial data may be held in a remote data centre with connections made via an Internet browser. As the application is provided by a third party company the School should be aware that in such circumstances the software supplier may have full access to personal data related to its staff and pupils held within its servers.

Data Protection Requirements

Schools are **legally responsible** as data controllers for ensuring all reasonable steps have been taken to protect and safeguard personal data including staff and pupil records. Simply asking whether a company is registered with the Information Commissioner's Office (ICO) for data protection and agreeing to the supplier's terms and conditions will not be deemed acceptable under the new regulation. Such action could result in fines being imposed on the School in the event of a data breach. As a minimum, schools should have a contract in place with all third party suppliers that hold the School's staff and pupil personal data, which clearly references both parties' obligations including data protection.

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties. Similarly, if a processor uses another organisation (ie a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the GDPR, and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

Source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

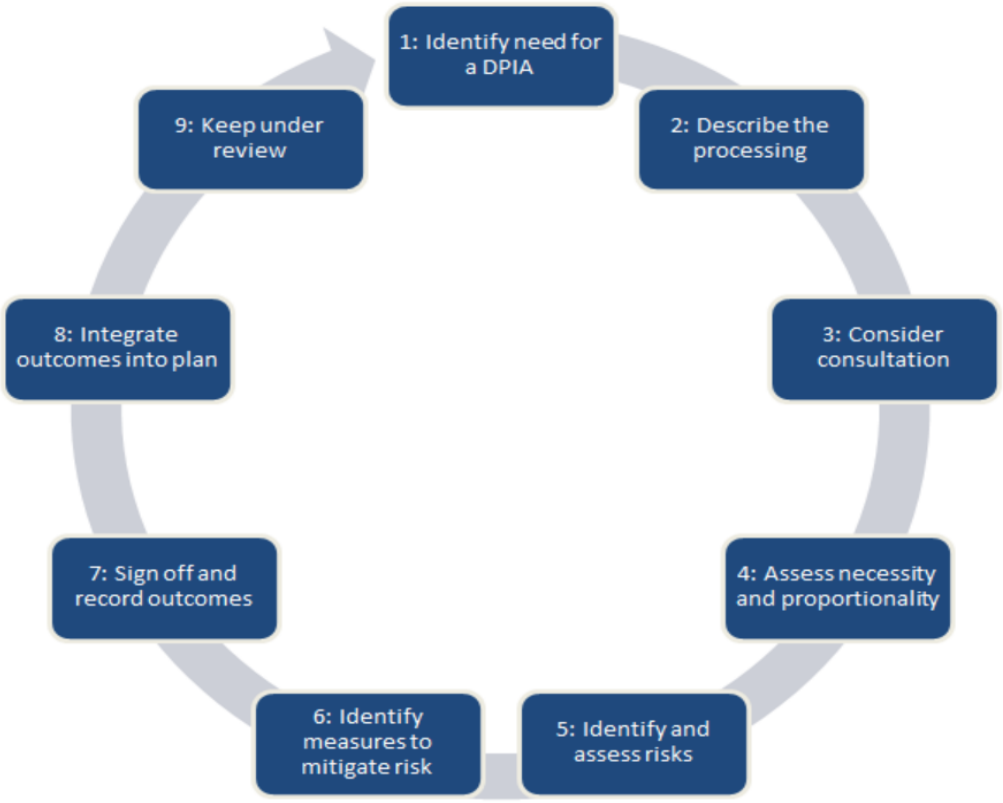
Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment is a process by which schools can identify and reduce the privacy risks of a particular task or project (i.e. procurement of new IT system). Whilst the use of DPIA is not a legal requirement in all areas where personal data processing is being undertaken (except 'high risk processing i.e. safeguarding data) it is recommended as a means to evidence that the School has appropriate controls in place. Examples where a DPIA should be used:-

- A new IT system for storing and accessing personal data;
- A data sharing initiative where two or more schools/ organizations seek to pool or link sets of personal data;
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring;
- Cloud hosted applications.

To provide transparency in the process, completed DPIAs should be reported to governors for review and approval.

A DPIA should begin early in the life of a project, before the start of any data processing, and run alongside the planning and development process. It should include the following steps:



Source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Selecting a Supplier

When selecting a supplier you should consider information security accreditations that the company may have as these provide an independent assurance that fundamental controls are in place. A number of the standards to be aware of are detailed below (list not exhaustive):-

- ✓ **PCI DSS.** (Payment Card Industry – Data Security Standard). Standard for organisations which store, process or transmit card holder information.
- ✓ **ISO27001:2013.** (Information Security Management Standard - ISMS). The ISMS includes information security policies and procedures.
- ✓ **Cyber Essentials Scheme.** Government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks.

It is expected that third party companies processing personal data should be accredited to the Cyber Essentials Scheme or equivalent as a minimum.

Helpful guidance from the Department for Education on the benefits and risks of moving information and services to the cloud can be found on the website link below:-

https://www.gov.uk/government/publications/cloud-computing-how-schools-can-move-services-to-the-cloud

IT System Procurement

At the start of the process it is essential that the School has a clear plan to consider the IT system procurement which outlines the key benefits, how these will be delivered and arrangements for meeting all associated costs. Consideration will also need to be given to evidencing value for money from the procurement i.e. 3 quotes/ or formal tender and that the system being assessed is compliant with current legislation. It is important to ensure that the Governing Body is aware of individual IT system procurements and, where appropriate, authorise their purchase. Training is an area which is frequently overlooked when procuring new IT systems and often leads to schools not fully utilising available functionality or achieving maximum efficiencies. It is useful to remember that where the County Council has a contract in place which includes schools, there is no need to obtain further quotes or undertake a formal tender process.

The Department for Education have prepared procurement advice and guidance to assist schools secure value for money and make the best use of resources. The information can be found at the following location

Buying for Schools
https://www.gov.uk/guidance/buying-for-schools

Deals for Schools
https://www.gov.uk/government/publications/deals-for-schools/deals-for-schools

At an early stage of the procurement the School should identify the likely timeframe by which the IT system or solution will be required e.g. 5 years. This will help to determine whether there is a requirement to undertake a formal tender process or simply invite three quotations on the basis of the total IT system spend. It is important to include 'added costs' such as training and support to obtain the overall cost figure. All documentation to support the procurement, including alternative suppliers considered as part of the process, should be retained in accordance with the School's document retention policy to evidence the decision taken and provide a clear audit trail.

On-line Payments System - Worked Example (Annual Charges)

Cost of system	£400
Support	£200
Annual Cost	£600
Training (Year 1)	£500
Total Annual Cost	£600 x 5 years + £500 = £3,500 (cost of the contract)

Any legal issues relating to the procurement or contract information should be referred to the Authority's Legal Services Division.

Contact: Mr Simon Macdonald-Preston
Telephone: (01629) 538290
Email: simon.macdonald-preston@derbyshire.gov.uk

Compliance with the Derbyshire Scheme for Financing Schools

Once a decision has been made to purchase an IT system, reference should be made to the Derbyshire Scheme for Financing Schools and the requirement for the County Council's Director of Finance & ICT to review new systems for the "maintenance of financial records or records of assets" (see extract below).

The Director of Finance and ICT shall approve any new systems for the maintenance of financial records or records of assets of the Authority, including schools, or any changes to such systems. All consultations relating to new systems or changes to existing systems should be undertaken through the Assistant Director of (Audit) who will consider the impact on the Internal Control Framework and report to the Director of Finance and ICT, raising any concerns as appropriate.

Systems which involve the processing of significant volumes of personal data e.g. pupil names, dates of birth, addresses etc. should also be notified to Audit Services in order that compliance with current data protection regulations can be assessed. Examples of such systems and the type/ nature of transactions are detailed below:-

Type of IT System	Notify Audit Services
Contains Staff, Parent or Pupil names, addresses, date of births etc. ✓ Management Information System (MIS); ✓ Safeguarding; ✓ Pupil Attainment.	✓
Collects or processes financial payments on behalf of the School ✓ Payment systems; ✓ Imprest systems.	✓
Contains School assets and inventory ✓ School Inventory systems.	✓
Educational support systems which contain ✓ Limited personal data i.e. pupil name and class number; ✓ Limited or no financial transactions.	X
Note: There are a range of methods by which IT systems can be installed including locally on the School's IT network or remotely using the cloud or other infrastructure.	

All referred IT systems which hold or process personal data will be assessed to determine the associated level of perceived risk to the school and the current number of schools using the application. The risk assessment is detailed in ***Appendix A***. Once a total risk score has been determined, Audit will assign one of three classifications; "Low Risk IT System", "Medium Risk IT System" or "High Risk IT System". The classification will drive the priority of the Audit review with High and Medium Risk IT systems prioritised and subject to the following:-

1. Assessment of the IT system;

2. Assessment of the data hosting location holding the school's information;

3. Assessment of the supplier's head office information security procedures.

Assessment of the IT system

The objective of the IT system review is to ascertain whether there is a baseline IT security control framework in place and to confirm that these controls form part of the 'live' system. The assessment will consider a number of areas including the application's password policy, data validation procedures, audit trail and management of user permissions. Reference to ISO27001:2013 security controls will be used as a guide in terms of effective information security procedures.

Assessment of the data hosting location holding the School's information

The objective of the Audit review of the supplier's data hosting arrangements is to evidence that effective information security processes and data protection procedures are operational to mitigate the risk of unauthorised access to, or loss of, the School's data. Where a site visit is considered necessary, Audit Services will seek assurances regarding the adequacy of the physical and environmental controls at the data centre, staff recruitment procedures, data disposal process, data encryption, schedule of

external penetration tests and local information security procedures. As Audit Services have no 'rights of access' to the data hosting network or servers, a number of controls can only be evidenced through discussion with the company's staff. In the event that the data hosting location can evidence certification against the ISO27001:2013 information security standard, this element of the review will not be undertaken.

Assessment of the Supplier's head office information security procedures

The objective of the Audit review of the Supplier's Head Office is to assess the level of compliance with information security best practice, data protection obligations and assess the level of risk to the School's data from the supplier's staff and/or local administrative procedures. During the site visit, Audit Services will seek to validate the level of compliance with a number of areas including information security policies and procedures, review staff recruiting processes, check the level of encryption applied to IT equipment, assess incident reporting mechanisms and physical security controls. Similar to the data hosting review a number of the controls can only be confirmed following discussions with the supplier's staff.

Application penetration or vulnerability testing

The objective of a penetration test is to assess the IT system's security protection by seeking to identify software weaknesses which could enable unauthorised access to the application or its data. Testing can be performed manually, with the use of an automated testing application or a combination of both. Other than tests that the company may have commissioned, Audit Services do not currently undertake any independent penetration or vulnerability testing of school IT systems.

Reporting of the Audit Findings

At the conclusion of the Audit review the information security issues are communicated to the supplier for review. At this point the Supplier has the opportunity to provide a comment to Audit Services on the issues that have been identified and include an appropriate response stating how the control weakness will be addressed (including a timeframe for correction). In the event that the Supplier's response is satisfactory, with an appropriate timeframe provided for the correction of the identified issues, the Director of Finance & ICT will be provided with an Audit report to consider the IT system's use. A detailed list of the suppliers who have been audited under this process is attached at **Appendix B** to this guidance.

In the event that a school selects a supplier who has completed the Audit assessment process, as detailed in Appendix B, the School should obtain an assurance from the supplier that any recommendations agreed with Derbyshire Audit Services have been implemented and maintained.

Audit Services Limitations and Disclaimer

The matters identified during the review of individual IT systems, suppliers, offices and data hosting facilities are only those which came to Audit's attention during the course of the assessment. It should be noted that they are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that may be made during

any contractual arrangements between the Supplier and the School. Audit Services work should not be taken as a substitute for Management's responsibilities for the implementation of an effective control environment.

Due to the nature of the Audit undertaken and the fact that Audit staff do not have any rights of access to the Supplier's administration processes a number of the responses can only be evidenced through discussions with company staff. Audit Services are also reliant upon the supplier implementing the agreed recommendations to address the matters identified during the Audit review within the notified timeframe. In the case of IT systems, approval is given in respect of the version of the software made available for testing.

Getting in Touch

Audit staff are always available to provide advice and support. If you have any specific queries on the content of this guidance or are considering implementing a new system that requires notification to Audit Services please get in touch.

Contact	Position	Email	Telephone
Philip Spencer	Audit Manager	philip.spencer@derbyshire.gov.uk	(01629) 539230
Jayne Wallhead Suzanne Kiernan	Audit Clerks	jayne.wallhead@derbyshire.gov.uk suzanne.kiernan@derbyshire.gov.uk	(01629) 538826

Appendix A
Information Security Risk and Impact Assessment

Score	Information Risk The level and nature of **special categories of personal data** and/or **personal data** as defined under the Data Protection Act 2018.
5 ☐	Safeguarding information and/or the IT solution includes **special categories of personal** and/or **personal** data records including: • racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health or data concerning a natural person's sex life or sexual orientation.
4 ☐	**Personal** data that when put together can be used to identify a natural person including, name, address, date of birth, gender, email, national insurance number etc. The IT solution also includes one of the following **special categories of personal** data records: • racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health or data concerning a natural person's sex life or sexual orientation.
3 ☐	**Personal** data that when put together can be used to identify a natural person including name, address, date of birth, gender, email, etc.
2 ☐	Limited **personal** data that when put together is unlikely to identify a natural person.
1 ☐	No personal data, which does not enable the identification of a natural person.

Information Risk Assessment - Scoring Range				
1	2	3	4	5
Low Risk IT System or Service		**Medium Risk IT System or Service**	**High Risk IT System or Service**	

Note: As a minimum financial applications including on-line payment solutions and inventory IT systems will be categorised as Medium Risk IT System.

Examples of expected data protection and information security controls for IT solutions or services where there is a requirement for the storing, handling, processing of personal data by third parties are detailed in **Appendix C** based on the risk ranking of the IT system or service above. The controls are aligned to the risk assessment above and provide Schools with a 'checklist' to discuss with suppliers based on the personal data being held. As the data controller it is the responsibility of all schools to ensure that third party suppliers have appropriate controls in place to protect their personal data.

Appendix B
Derbyshire Audit Services - Assessment of School IT Systems and Providers

Important Note

Inclusion within the Derbyshire Audit Services 'Audit Guidance for Schools on the Procurement of IT Systems' does not in any way constitute endorsement of any supplier or IT system. Neither the County Council nor its staff are responsible for making recommendations on the suitability of IT systems for use within schools or whether they will deliver the perceived benefits. Such evaluations must be made by school management and Governors in accordance with the School's financial procedures and legal obligations. In the event that a school selects a supplier who has completed the Audit assessment process, as detailed below, the School should obtain an assurance from the supplier that any recommendations agreed with Derbyshire Audit Services have been implemented and maintained.

Suppliers who have Completed the Audit Assessment									
Supplier	**System**	**System Type**	**Assigned System Risk**	**Data Centre Audit**	**Head Office Audit**	**Application Testing**	**Application Penetration Testing**	**Reported to Director of Finance & ICT**	**Follow Up Review**
Capgemini	SAP Finance *(DCC Contract in place)*	Finance System	High	✓	✓	✓	No	April 2014	Managed by DCC
RM Education Ltd	Integris *(DCC Contract in place)*	Management Information System	Medium	✓	✓	✓	No	July 2015	ISQ Issued
Results Squared Limited	School Asset Manager	Inventory	Low	Note 1	Note 1	✓	No	December 2014	ISQ Issued
ParentPay	ParentPay *(DCC Contract in place)*	On-line Payments	Medium	✓	✓	✓	No	July 2015	ISQ Issued
InVentry	School Audit Inventory	Inventory	Low	Note 1	Note 1	✓	No	June 2016	ISQ Issued
Teachers2Parents	School Money	On-line Payments	Medium	✓	✓	✓	No	July 2016	ISQ Issued

Appendix B
Derbyshire Audit Services - Assessment of School IT Systems and Providers

Suppliers who have Completed the Audit Assessment									
Supplier	**System**	**System Type**	**Assigned System Risk**	**Data Centre Audit**	**Head Office Audit**	**Application Testing**	**Application Penetration Testing**	**Reported to Director of Finance & ICT**	**Follow Up Review**
OneTeam Logic	MyConcern	Safeguarding	High	Note 2	✓	✓	No	July 2016	ISQ Issued
Tucasi Ltd	School's Cash Office	On-line Payments	Medium	✓	✓	✓	No	October 2016	ISQ Issued
Meritec Ltd	CPOMS	Safeguarding	High	✓	✓	✓	No	October 2016	ISQ Issued
Cool Milk at School Ltd	CoolMilk	Free/Subsidised Milk	Medium	✓	✓	✓	No	December 2017	ISQ Issued
Clifton EMAG Ltd	Eaz Mag	Pupil Attainment	Medium	Note 3	✓	✓	No	March 2017	ISQ Issued
OTrack	School Assessment	Pupil Attainment	Medium	Note 4	✓	✓	No	May 2017	ISQ Issued
123Comms Ltd	ParentMail	On-line Payments	Medium	Note 4	✓	✓	No	July 2017	ISQ Issued
Nexus Software Platforms Ltd	Parenthub	Parent Engagement	Medium	Note 4	✓	✓	No	December 2017	ISQ Issued
Maths Circle Ltd	Times Tables Rock Stars	Support Times Table Knowledge	Low	A full Audit was not required as the supplier agreed to remove the personal data being captured by Derbyshire schools, which reduced the data protection compliance level.			No	Jan 2018	N/A
Insight Tracking	Insight Pupil Assessment	Pupil Attainment	Medium	Note 4	✓	✓	No	January 2018	ISQ Issued

Appendix B
Derbyshire Audit Services - Assessment of School IT Systems and Providers

Suppliers who have Completed the Audit Assessment									
Supplier	**System**	**System Type**	**Assigned System Risk**	**Data Centre Audit**	**Head Office Audit**	**Application Testing**	**Application Penetration Testing**	**Reported to Director of Finance & ICT**	**Follow Up Review**
2 Eskimos Ltd	2Eskimos	Reading Assessment	Medium	Note 4	✓	✓	No	April 2018	ISQ Issued
Angel Solutions	Balance	Pupil Attainment	Medium	Note 4	✓	✓	No	June 2018	ISQ Issued
Cornerstones Education Limited	Cornerstones	Pupil Attainment	Medium	Note 4	✓	✓	No	June 2018	ISQ Issued
SafeGuard Software Limited	Safeguard	Safeguarding	High	Note 4	✓	✓	No	July 2018	ISQ Issued
Sandgate Systems Ltd	Every	Asset Management	Low	Note 4	Note 1	✓	No	July 2018	ISQ Issued
Schoolcomms	Schoolcomms	On-line Payments	Medium	Note 4	✓	✓	No	August 2018	ISQ Issued
Wonde Ltd	Wonde	Data extraction Tool	High	Note 4	✓	✓	No	June 2019	2020

ISQ – Supplier has been asked to complete the County Council's expected controls matrix to evidence level of compliance.
Note 1 – System contains limited personal information or has low overall financial risk.
Note 2 – Data Centre does not permit third party access or reviewed under a separate Audit.
Note 3 – The data centre currently used by the company is in the process of obtaining ISO27001:2013 certification.
Note 4 – Data hosting environment holds current ISO27001 certification and there Audit site visit was not undertaken.

Appendix B
Derbyshire Audit Services - Assessment of School IT Systems and Providers

SAP Interfaces into School's SAP Finance System

At the completion of the Audit Assessment on-line payment suppliers are provided with the contact details for the SAP Development Team to discuss the process of enabling the on-line payment system to interface directly into the school's SAP accounts and remove the requirement to process cash journals. As at 28 June 2019:-

1.	ParentPay	ParentPay	Interfaces directly into school's SAP accounts
2.	Teachers2Parents	School Money	Supplier notified, although SAP Development Team are awaiting a response
3.	Tucasi Ltd	School's Cash Office	Supplier notified, although SAP Development Team are awaiting a response
4.	123Comms Ltd	ParentMail	Supplier notified, although SAP Development Team are awaiting a response

In the event that the school chooses an on-line payment supplier for the receipt of public monies (i.e. school meals) which currently does not interface into the school's SAP accounts then the system must be configured to use the school's Imprest account.

Important Note

Inclusion within the Derbyshire Audit Services 'Audit Guidance for Schools on the Procurement of IT Systems' does not in any way constitute endorsement of any supplier or IT system. Neither the County Council nor its staff are responsible for making recommendations on the suitability of IT systems for use within schools or whether they will deliver the perceived benefits. Such evaluations must be made by school management and Governors in accordance with the School's financial procedures and legal obligations.

Appendix B
Derbyshire Audit Services - Assessment of School IT Systems and Providers

Suppliers who are currently in the Process of completing the Audit Assessment									
Supplier	**System**	**System Type**	**Assigned System Risk**	**Data Centre Audit**	**Head Office Audit**	**Application Testing**	**Application Penetration Testing**	**Reported to Director of Finance**	**Follow Up Review**
Audit Services are in the process of contacting various Suppliers to arrange site visits over the School holidays.									

***N/A – System contains limited personal information or has low overall financial risk.**

****Not Tested – Data Centre does not permit third party access or reviewed under a separate Audit.**

Appendix C
Derbyshire Audit Services - Assessment of School IT Systems and Providers

BACKGROUND

This document sets out the guidance on the minimum data protection and information security controls for IT solutions or services where there is a requirement for the storing, handling, processing or retention of personal data by third parties (including suppliers, contractors, sub-contractors and employees). The expected controls aim to protect the School's interests by providing a flexible approach to managing data protection and information security risks during contractual arrangements. The term **'Data'** within Appendix C refers to the storing, handling, processing or retention of **personal data** or **special categories of personal data** related to the School's information e.g. employees, pupils, parents and volunteers.

1.	**Expected Control - Human Resource Security**	**Restricted Data**	**Controlled Data**	**Public Data**
1.1	Staff with access to the **Data** must have a written contract of employment under which they agree to adhere to information security policies, including a staff acceptable use policy.	✓	✓	X
1.2	Staff with access to the **Data** must receive an induction and have a continuous training programme that includes information security and data protection guidance throughout their employment.	✓	✓	X
1.3	Staff must not transfer the **Data** to personal email accounts or personal cloud based storage.	✓	✓	X
2.	**Expected Control - Physical and Environmental Security**	**Restricted Data**	**Controlled Data**	**Public Data**
2.1	The infrastructure hosting the **Data** must be classified as Tier 2 or above.	✓	X	X
2.2	The infrastructure hosting the **Data** must be certified to the information security standard ISO27001:2013 or equivalent.	✓	X	X
2.3	Physical access procedures must be in place to control access to sites hosting the **Data** to reduce the risk of unauthorised access, damage or theft and include:- • Visitor signing in procedures; • CCTV coverage of exit/entry points and data hosting environments; and • Alarm systems (including environment sensors) covering the hosting environment of the solution.	✓	✓	X

Appendix C
Derbyshire Audit Services - Assessment of School IT Systems and Providers

3.	Expected Control – Access Security	Restricted Data	Controlled Data	Public Data
3.1	IT solutions that record or process the **Data** must ensure that:- • Individual accounts are granted with minimum privileges to provide the service; • Default accounts are deleted or disabled; • Privileged account access is logged and periodically reviewed; • Reports are available on disabled, suspended and in-active users; • Access to the IT solution's audit trail is restricted and controlled; • Access to IT solution's source code is restricted and controlled; and • Access to information systems audit tools is restricted to prevent misuse or compromise e.g. password cracking tools and vulnerability scanning software.	✓	✓	✓

3.2	All IT solutions processing the **Data** must have a configurable system-enforced password and user account policy, which includes:-
	• Configurable password history;
	• Configurable maximum password age;
	• Configurable minimum password age;
	• Configurable minimum password length (minimum of 8 characters);
	• Configurable complexity requirements of at least four of the following elements:
	  ○ Numeric – (0-9)
	  ○ Uppercase – (A-Z)
	  ○ Lowercase – (a-z)
	  ○ Special Characters (?,!, @, #, %, etc…)
	  ○ Spaces
	• Configurable account lockout threshold of invalid logon attempts.
		✓	✓	✓

3.3	IT devices accessing the **Data** must have an automated lockout if left unattended or idle for a period of 10 minutes.	✓	✓	X
3.4	System and administrative accounts must have the ability to be changed without resulting in changes to software coding.	✓	✓	✓
3.5	IT Solutions processing the **Data** must have the ability to enable two factor authentication if required.	✓	✓	X

Appendix C
Derbyshire Audit Services - Assessment of School IT Systems and Providers

4.	Expected Control - Network and Infrastructure Security	Restricted Data	Controlled Data	Public Data
4.1	The Company must hold a current 'Cyber Essentials Plus' certification (or equivalent) 	✓	X	X
4.2	The Company must hold a current 'Cyber Essentials' certification (or equivalent) 	X	✓	X
4.3	Networks hosting the **Data** must be held within an authenticated, secure network domain boundary.	✓	✓	✓
4.4	The IT solution must be segregated on networks by the implementation of either physically different networks, or use of logical networks (e.g. virtual private networking), in order to protect the **Data** within the solution.	✓	✓	X
4.5	IT solution(s) and devices hosting/ accessing the **Data** must run up to date anti-virus and malware protection software.	✓	✓	✓
4.6	The IT solution should have the ability to encrypt sensitive data before storage within the database.	✓	✓	X
4.7	Regular backups of the **Data** must be undertaken and encrypted to at least AES 128 standard or equivalent.	✓	✓	X
4.8	Auditing of activities in the **Data** hosting environment must be kept secure and protected against alteration or deletion.	✓	✓	✓
4.9	Intrusion detection strategies must be in place, which include regular penetration testing.	✓	✓	X
4.10	Patch management procedures must be in place to ensure security bug/fixes are applied to all IT solutions hosting the **Data** and are in accordance with the vendors recommended guidance.	✓	✓	✓
4.11	IT devices (including laptops & PCs) used to store or process the **Data** must be protected using whole disk encryption to at least AES 128 standard or equivalent.	✓	✓	X
4.12	Obsolete IT devices used to record, store or process the **Data** must be securely wiped to render the data unrecoverable.	✓	✓	X
4.13	Passwords used to encrypt IT devices and solutions holding the **Data** must meet the following complexity requirements:- • Minimum password length **8** characters;	✓	✓	X

	• Include complexity requirements of at least four of the following five elements: ○ Numeric – (0-9) ○ Uppercase – (A-Z) ○ Lowercase – (a-z) ○ Special Characters (?,!, @, #, %, etc…) ○ Spaces			
4.14	The **Data** must be transferred/exchanged via secure communication channels which are protected by a minimum of TLS v1.2 protocol (or equivalent) that enables as a minimum 256-bit symmetric key encryption using SHA256RSA signature algorithm with RSA public asymmetric key encryption of 2048 bits.	✓	✓	X
4.15	The **Data** must be encrypted to at least AES 128 standard or equivalent, whilst at rest within the hosting environment.	✓	✓	X
5.	**Expected Control - System Acquisition, Development and Maintenance**	**Restricted Data**	**Controlled Data**	**Public Data**
5.1	IT solutions development and maintenance procedures must be in place to ensure information security is an integral part of IT solution development.	✓	✓	X
5.2	Any IT solutions or hardware installed onto the Council's IT infrastructure must be supported by documentation, which details the running environment, installation procedures and any known issues that may adversely affect the security and integrity of the Council's information.	✓	✓	✓
5.3	A separate test environment must be available to replicate the live system to facilitate assessments and development which will not put the Council's IT network at enhanced risk.	✓	✓	X
5.4	'Live' **Data** must not be used in test systems.	✓	✓	X
5.5	Procedures must be in place to enable the secure transfer of the **Data** from the Council's existing IT solution to the supplier's hosting environment during the implementation phase including data validation, data migration and customisation phases.	✓	✓	X
5.6	The integrity, confidentiality and availability of the **Data** must be maintained during the decommissioning of IT solutions and when moving to a new solution/system.	✓	✓	X
5.7	IT solutions processing the **Data** must have an extractable audit trail which will record the activity of users and system administrators including:-	✓	✓	✓

	• Date and time of transaction; • User ID and name of the individual undertaking the transaction; • Details of the data before and after the transaction; and • Details of the user's MAC or IP address (subject to whether the connection is internal or external) of the IT equipment for the user making the connection.			
5.8	IT solutions processing the **Data** should have a configurable welcome page to remind users of their obligations when accessing the system.	✓	✓	✓
5.9	To enable continuity of service, procedures should be in place to enable the transfer of **Data** to the Council or new contractor at the end of a contract period.	✓	✓	✓
5.10	IT solutions processing or holding the **Data** must have procedures in place to enable the Council to comply with its local data retention policies and legal obligations.	✓	✓	✓
6	**Expected Control - Business Continuity Management**	**Restricted Data**	**Controlled Data**	**Public Data**
6.1	Procedures must be in place to enable the recovery of IT solutions including user data and/or credentials in the event of interruption to normal operational service.	✓	✓	✓
6.2	Physical and logical access controls must be in place to maintain the security of the **Data** to an equivalent standard to that within the 'live' environment during the business recovery process.	✓	✓	✓
7.	**Expected Control - Expected Controls - Information Security Incident Management and Compliance**	**Restricted Data**	**Controlled Data**	**Public Data**
7.1	An information security management procedure must be in place, including a clear method by which information security incidents are notified to the Council.	✓	✓	✓
7.2	The knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	✓	✓	✓
7.3	Details of information security events/ breaches related to the processing of the **Data**, must be kept secure and protected against alteration or deletion.	✓	✓	✓
7.4	Compliance is required with the following in respect of the **Data**: • General Data Protection Regulations and Data Protection Act (2018); • The Computer Misuse Act (1990);	✓	✓	✓

	• The Electronic Communications Act (2000); • Privacy and Electronic Communications Regulations (2015); and • The Copyright, Designs and Patents Act (1988).			
7.5	Procedures should be in place for third parties to conduct audits of supplier services to ensure that information security, data protection terms and conditions are being adhered to.	✓	X	X

Additional guidance or clarification on the requirements within **Appendix C** can be obtained from the Council's Information Security Team using the following contact details:

Telephone: (01629) 538984 **Email: security.team@derbyshire.gov.uk**