



Policy Name	DATA PROTECTION
Relevant To	Federation <input checked="" type="checkbox"/> Bidwell Brook Only <input type="checkbox"/> Ellen Tinkham Only <input type="checkbox"/>
Type of Policy	Model <input type="checkbox"/> School <input checked="" type="checkbox"/>
Name of Policy Holder	Dave O'Loughlin
Subject/Department	GDPR
Approved By	Full Governing Body <input type="checkbox"/> CBT Governors <input checked="" type="checkbox"/> T&L Governors <input type="checkbox"/> SLT <input type="checkbox"/>
Version Date (if applicable)	1.0
Date of Last Review	Summer Term 2024
Date of Next Review	Summer Term 2025

1. Introduction

- 1.1 This policy outlines the framework that governs how the Learn to Live Federation and its staff must handle personal data to ensure compliance with the [Data Protection Act 2018](#) and associated data protection laws applicable in the UK.

2. Scope

- 2.1 This policy applies to the processing of personal data which is defined by [Part 1, Section 3](#) of the Data Protection Act 2018 and to the processing of special categories of personal data defined by [Part 2, Chapter 2](#) of the Data Protection Act 2018.
- 2.2 This policy and its supporting guidance shall apply to all Learn to Live Federation employees, agency and temporary staff, contractors, members and third-party staff, who have access to information systems or information used for School purposes.
- 2.3 Where this policy reads "staff", it should be read to include all the entities in paragraph 2.2.

3. Legislation

- 3.1 The Learn to Live Federation processes a variety of personal data to enable us to deliver a range of education services. Therefore, the Learn to Live Federation is required to comply with the GDPR as well as other supporting legislation which governs the processing of personal data.
- 3.2 When handling and managing information the School and its staff shall comply with other legislation in addition to the GDPR, to include but not limited to:
 - [Computer Misuse Act 1990](#)
 - [Copyright Designs and Patents Act 1988](#)
 - [Environmental Information Regulations 2004](#)
 - [Equality Act 2010](#)
 - [Freedom of Information Act 2000](#)
 - [Human Rights Act 1998](#)
 - [Local Government Act 1972](#)
 - [Local Government Act 2000](#)
 - [Regulation of Investigatory Powers Act 2016](#)
 - [Re-use of Public Sector Information Regulations 2005](#)

4. Breach of this Policy

- 4.1 All reckless or deliberate breaches of this policy will be investigated and may be referred to the Human Resources Department who will consider whether disciplinary action should be taken against the member of staff concerned. Alleged breaches of this policy will also be investigated by the Data Protection Officer as an information security incident in accordance with the Security Incident Management Policy and Procedure and may also be referred to Human Resources and senior management as considered necessary.

5. Policy Review

- 5.1 This policy will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer, Christine Walker contact christine.walker@learntolivefederation.co.uk (from September 2024).

6. Responsibilities

- 6.1 Responsibility for GDPR compliance rests with the Executive Head. The Data Protection Policy and its supporting guides and standards are managed, maintained and communicated to staff by the Data Protection Officer.
- 6.2 The School's Information Asset Owners and Information Asset Administrators are responsible for ensuring that appropriate structures and procedures are in place to manage their information effectively. They are also responsible for ensuring that staff are made aware of, and comply with this policy, its associated standards and procedures. All staff are personally responsible for complying with this policy and supporting standards.

7. The Data Protection Principles

- 7.1 The GDPR is underpinned by six common-sense principles which governs the way that the Learn to Live Federation must process personal data. These principles are outlined in [Part 4, Chapter 2](#) of the Data Protection Act 2018 and are summarised below.
- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
 - Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal/ data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
 - Personal data shall be kept for no longer than is necessary for the purpose for which it is processed.
 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational/ measures ('integrity and confidentiality').
- 7.2 Sections 8 - 20 outlines the steps that staff must follow when processing personal data to ensure compliance with each of the principles listed above.

8. Lawful Processing of Personal Data

8.1 The Learn to Live Federation and its staff must process personal data fairly and will not process personal data or special categories of personal data unless one or more of the lawful grounds listed in the Federation Privacy notices apply.

9. Privacy Notices

9.1 When collecting personal data, the Learn to Live Federation will make available the information contained in our template Privacy Notice. This may be available online and referenced on data capture forms, directly referenced on documentation or provided verbally. If Learn to Live Federation receives personal data from third parties, we will ensure that the information contained in a privacy notice, is made available to a data subject as soon as practical. This will usually be at the first point we are required to communicate with the data subject.

9.2 Privacy Notices are available on the Bidwell Brook School, Ellen Tinkham School and Learn to Live Federation websites. For more detailed assistance contact the Data Protection Officer.

10. Consent

10.1 The Learn to Live Federation is only required to obtain someone's consent if there is no other legal basis for processing their personal data. If we are required to obtain consent, we will ensure that the following requirements are met:

- The consent is freely given
- The person giving consent understands fully, what they are consenting to
- There must be a positive indication of consent (opt-in as opposed to opt-out)
- The person giving consent must be able to withdraw their consent at any time
- Consent should be documented so that it may be referred to in the future, if necessary

10.2 Children under the age of 13 merit specific protection regarding their personal data. Such specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data regarding children when using services offered directly to a child. If the Learn to Live Federation is required to deliver such services to children, it will ensure that the requirements of [Part 2, Chapter 2, Section 9](#) of the Data Protection Act 2018 are met.

11. Rights of data subjects

11.1 [Part 2, Chapter 2](#) of the Data Protection Act 2018 outlines the rights afforded individuals in respect of the processing of their personal data. These rights are summarised below:

- The right to transparency in respect of the processing of their personal data
- The right of subject access
- The right to rectification
- The right to erasure
- The right to restriction of processing

- The right to data portability
 - The right to object to processing
 - The right to request human intervention if processing is by automated means
- 11.2 Requests to exercise any of these rights are managed by the Data Protection Officer. The school's procedures for managing such requests are available on the Learn to Live Federation website and shall be adhered to whenever the Learn to Live Federation receives a request from someone wishing to exercise these rights.
- 11.3 When designing, implementing or procuring systems or services, the Learn to Live Federation must ensure that those systems or services can allow members of the public to exercise any of the rights listed in section 11.1. Any systems or services found to be incapable of managing such requests, should be referred to the Data Protection Officer.

12. Privacy by Design

- 12.1 [Part 3, Chapter 4, Section 57](#) of the Data Protection Act 2018 creates a statutory obligation on the Learn to Live Federation to ensure that a privacy impact assessment is undertaken on all new systems, processes or procedures that intend to process personal data, prior to their implementation. Such assessments are to be carried out by or in consultation with the Data Protection Officer. All assessments undertaken will be carried out in accordance with the School's Privacy Impact Assessment Procedure.
- 12.2 Compliance risks identified following a privacy impact assessment will be presented to relevant Information Asset Owners, Information Asset Administrators and or the Senior Information Risk Owner (SIRO) in accordance with the School's Information Assurance Policy.
- 12.3 If following the completion of a privacy impact assessment, the Learn to Live Federation identifies processing activities assessed as high risk that cannot be mitigated to an acceptable level, the authority will consult with the Information Commissioner's Office prior to implementing the proposed processing activity, system or process.

13. GDPR and Procurement

- 13.1 The Learn to Live Federation is committed to upholding the confidentiality, availability and integrity of information that is processed by our contractors on our behalf. Underpinning this commitment, we will ensure that the following measures are followed when procuring goods and services that involve the processing of personal data.

A privacy impact assessment is undertaken prior to any procurement which involves the processing of personal data.

A security questionnaire is completed to ascertain the technical and organisational measures that prospective contractors will put in place to protect the data that they will processing on behalf of the Learn to Live Federation. The results of which will inform on the final decision as to whether the school contracts with that organisation.

When procuring goods and services that requires a formal procurement exercise, we will ensure that contractual provision is in place which clearly identifies the following; who is the data controller; what data is being processed; a record of processing activity (in accordance with [Part 3, Chapter 4, Section 61](#) of the Data Protection Act 2018); arrangements for how personal data will be disposed of or returned to the School at the end of the contract; contractual clauses which mandate conformance to the GDPR.

When procuring goods and services that do not require a formal procurement exercise, and which involve the processing of personal data, staff must consult with the Data Protection Officer and the ICT Manager at their local setting.

- 13.2 Where risks are identified during a formal or informal procurement process, these will be managed in accordance with the School's Information Assurance Policy.

14. Records of Processing Activity

14.1 Information Asset Owners will ensure that records of the processing activity are maintained for all information assets under their direct responsibility. Such records will include the information required in [article 30](#) of the GDPR. Such records are to be made available to members of the public, the Information Commissioner's Officer (or other supervisory authority as required) or the European Data Protection Board (if still relevant post Brexit) on request.

14.2 The Learn to Live Federation will have measures in place to ensure that data processors responsible for processing personal data on behalf of the school, will maintain records of processing as required by [Part 3, Chapter 4, Section 61](#) of the Data Protection Act 2018.

15. Security Incident Management and Notification

15.1 An information security incident can occur when the confidentiality, availability and or integrity of personal data is put at risk. Examples of activities considered an information security incident might include; information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the School; sold or used without the permission of the School or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

15.2 The Learn to Live Federation has an Appendix C in place which governs how the school and its staff must report and handle incidents. This policy and procedure must be followed at all times.

15.3 In accordance with [Part 3, Chapter 4, Section 67](#) of the Data Protection Act 2018, the Learn to Live Federation is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours, of being notified of an information security incident that might adversely affect the rights and freedoms of a data subject. Notifications of this nature are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and where appropriate escalated in accordance with the School's Information Assurance Policy.

16. The Data Protection Officer

- 16.1 [Part 3, Chapter 4, Section 69](#) of the Data Protection Act 2018 requires that the Learn to Live Federation appoints a Data Protection Officer to undertake the tasks outlined in [Part 3, Chapter 4, Section 71](#) of the Data Protection Act 2018. Contact details for the Data Protection Officer will be made publicly available and will be referred to in all privacy notices.
- 16.2 The Learn to Live Federation will commit to ensure that the Data Protection Officer is sufficiently resourced to undertake the tasks assigned to them under [Part 3, Chapter 4, Section 71](#) of the Data Protection Act 2018. The school will also ensure that the Data Protection Officer is consulted on all matters which concern the processing of personal data.
- 16.3 The Data Protection Officer will act as the single point of contact for the Information Commissioner's Office or other relevant supervisory authorities and will ensure that compliance risks are reported to the highest level of management within the Learn to Live Federation as required.

17. Transfers Outside the European Economic Area

- 17.1 As we do not routinely transfer data either into or outside the European Union, we do not need to make any adjustments to our current policy.

18. Information and Cyber-Security

- 18.1 The Data Protection Officer is responsible for the creation and communication of guidance on information security. This guidance will be routinely reviewed to ensure accuracy, with amended and new guidance communicated to staff on a regular basis.
- 18.2 Staff who are required to process personal data, in whatever format, must ensure that they follow the relevant guidance on information security. If it is found that this guidance has not been followed, this will be treated as an information security incident and will be investigated in accordance with the Security Incident Management Policy and Procedure. Where such actions are considered negligent, reckless or malicious, this will be referred to Human Resources for consideration as to the merits of disciplinary action.
- 18.3 Should it be considered necessary for staff to be excused from following the requirements outlined in any guidance on information security, these requests will be the subject of a privacy impact assessment.

19. Sharing Personal Information

- 19.1 The Learn to Live Federation will only share personal data contained in its records with individuals who have a legitimate and legal right to view or receive it. Disclosures of personal data shall be proportionate and necessary and made in line with the School's policies and procedures. All disclosures shall comply with the [Data Protection Act 2018](#) and associated data protection legislation, [Human Rights Act 1998](#) and Common Law Duty of Confidence.

20. Information Assurance, Compliance and Reporting

- 20.1 The Learn to Live Federation will have in place, an information assurance framework to aid in the identification, management and ownership of information risks. This framework is outlined in the School's Information Assurance Policy.
- 20.2 All information risks identified when working with services, following privacy impact assessments or from information security investigations, will be managed in accordance with the Information Assurance Policy. Compliance risks that are identified will be monitored by the Data Protection Officer and reported on a regular basis, to Information Asset Owners, Information Asset Administrators and to the Senior Information Risk Owner (SIRO).

21. Policy History

- 21.1 This Policy is maintained by the Data Protection Officer and will be reviewed on an annual basis. For help in interpreting this policy, contact Christine Walker, christine.walker@learntolivefederation.co.uk



APPENDIX A

GDPR - DOCUMENT HANDLING PROTOCOL

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This protocol relates to the handling of any physical document within the Learn to Live Federation which contains the personal data of any individual.

It is expected that physical documents will only be produced when there is no other practical alternative. Electronic storage of personal information is the preferred method.

Examples of personal information are:

- Name
- DOB
- Contact details
- Medical conditions
- Initials

Documents will be classified depending on the amount and type of personal data they contain and should be produced, stored and disposed of appropriately. Categories are:

LEVEL ONE

Limited personal information, for example lesson plans with pupil's initials, names, Home School Diaries.

LEVEL TWO

More detailed personal information, including anything with full personal information along with contact details.

LEVEL THREE

Full personal information, including medical details, behaviour plans, manual handling plans, staff personal files and any information that falls into the "special categories" of data defined by the GDPR, these being:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

If you are unsure of the classification of a document, you should classify it in the highest category you think appropriate.

The following table details how different categories of data will be produced, handled and disposed of:

Category	LEVEL ONE	LEVEL TWO	LEVEL THREE
Who can produce/print document?	Any member of staff who has a reasonable reason to produce this type of document.	Teachers and any admin/support staff who has a reasonable reason to produce this document.	These documents can only be produced by authorised staff.
How should production be recorded?	Production does not need to be recorded but staff need to be aware that personal information is contained in the document.	Production does not need to be recorded but staff should try and avoid producing a hard copy unless there is no alternative. Staff also need to be aware that this document contains more detailed personal information.	Production will be recorded in a log, this log will detail the distribution of these documents.
How should document be stored?	The document can be stored anywhere in the school but consideration should be given to any other users of the school, for example hirers of the hall, after school club etc.	Document should be in a locked container when not in use.	Document should be in a locked container when not in use.
How should the document be disposed of?	Document should be disposed of as confidential waste.	Document should be disposed of as confidential waste.	Document should be returned to the producer when no longer required so that its destruction can be recorded.
What to do in the event of a data breach?	If it is known that a document has been lost this should be reported to the DPO.	If it is known that a document has been lost this should be reported to the DPO who will decide if the breach needs to be reported to the ICO.	If a document is lost the DPO will carry out an investigation and report the loss to the ICO.

DPO = Christine Walker; ICO = Information Commissioner's Office



DOCUMENT FILING

A key requirement of the GDPR is the right to the return of or destruction of any personal data which is held on an individual. To facilitate this, documents are to be held in a way which allows us to easily identify all the information we hold on a pupil or member of staff. The easiest way to achieve this is to have a single file on each pupil or member of staff. However, it is recognised this may not always be a practical solution in which case information can be held in separate files as long as they are easily identifiable. In the event of a separate file no longer being necessary, the information contained within it should be returned to the pupil or staff member's main record.



APPENDIX B

ELECTRONIC DATA PROCEDURE

Under GDPR we have a responsibility to ensure that personal data:

- is kept secure;
- is accurate;
- can be destroyed on request;
- can be transferred on request;
- can be viewed on request.

To allow us to comply with GDPR the following procedures are in place and should be adhered to:

- There will be a master folder for each pupil, all documents which contain any personal information about a student should be held in this folder or a subfolder within this folder.
- Personal information should never be transferred to a memory stick or any other type of removable storage unless absolutely necessary, any media used must be password protected.
- Personal data should never be sent to or shared with anyone outside the Learn to Live Federation unless this sharing is permitted within the relevant privacy notice. If you aren't sure, don't send.
- Any school IT equipment that you have access to should only be used for work related activity and must be protected by a suitable password. These devices should be kept physically secure when not in use.
- The use of personal equipment to access pupil or staff personal information (including that which may be contained in emails) is discouraged. If however it is felt that this is necessary the following must be adhered to:
 - The device must be password protected.
 - The device must be set to lock after no more than two minutes inactivity.
 - The device should not be shared with other people – even within a family.
 - In the event of a device which may contain personal data being lost or otherwise compromised, this loss should be reported to the DPO immediately.
- When a student is no longer in your class or you are no longer dealing with their data to provide other advice (manual handling, behaviour support, SALT etc), you should carry out a sweep of your personal folders to ensure that you have not inadvertently created any files containing their information. Any files found should be moved (not copied) to the relevant master folder.
- If you believe that you may have lost a device containing personal information or think that you may have shared information inappropriately, this should be immediately reported to the DPO.

**REMEMBER - PERSONAL DATA SHOULD BE TREATED AS PERSONAL PROPERTY.
TREAT THE DATA WE HOLD IN THE SAME WAY YOU WOULD LIKE OTHER PEOPLE
TO TREAT YOUR OWN INFORMATION.**



APPENDIX C

GDPR – SECURITY INCIDENT/DATA LOSS MANAGEMENT PROTOCOL

In order to comply with the requirements of the GDPR we are required to record and investigate any security incident or data loss.

WHAT IS A SECURITY INCIDENT?

An information security incident can occur when the confidentiality, availability and or integrity of the Learn to Live Federation's information is put at risk.

Examples of activities considered an information security incident might include:

- Information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the Learn to Live Federation; sold or used without the permission of the Learn to Live Federation or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

Other examples of information security incidents might include:

- losing paper files or documents containing personal or sensitive business data;
- faxing or emailing personal or sensitive business data to the wrong recipients;
- posting personal or sensitive business data to the wrong recipients;
- deliberately or accidentally disclosing personal or sensitive business data to people who are not legally entitled to the information;
- using or selling personal or sensitive business data without the permission of the Learn to Live Federation;
- deliberately or accidentally sharing a password or entry code to an office, computer system or files containing personal or sensitive business data, to someone who is not ordinarily entitled to see the information;
- computer equipment containing personal or sensitive business data is lost or stolen;
- a business-critical system containing personal or sensitive business data malfunctions and the information cannot be retrieved quickly;
- computer viruses, malware attacks or phishing scams against the IT systems;
- unauthorised access or attempted access to IT systems or secure areas.



WHEN TO REPORT

Any security incident, suspected security incident or near miss should be reported to the Data Protection Officer as soon as possible. In the absence of the Data Protection Officer being available, the incident should be reported to any member of the Senior Leadership Team.

Do not delay reporting an incident whilst you look for the lost information, report the loss as soon as it is identified.

HOW TO REPORT

If the incident relates to pupil or parent information it can be reported via CPOM's using the Data Loss category. If the incident relates to staff data or multiple pupils it should be logged within CPOMs, Data Loss category against "No Pupil".

LOGGING A SECURITY INCIDENT

The Data Protection Officer is responsible for overseeing information security incidents, upon being notified of an incident the following steps will be taken:

- The incident will be logged in the Learnt to Live Federation's incident log – kept on the CPOMs system;
- The Data Protection Officer will acknowledge receipt of the incident within two working days;
- Sufficient evidence to enable a risk assessment or privacy impact assessment to be gathered within two working days;
- An assessment of the severity of the incident to be carried out within three working days;
- Notify the Executive Head and relevant Governor if the incident will require reporting to the Information Commissioner's Office or if other appropriate action needs to be taken.

Every incident will be categorised according to the nature of the incident, the sensitivity of the data involved and the number of data subjects affected. If this is not immediately apparent it will be established during the investigation.

If a particular individual or team are repeatedly causing the same type of incident this will be referred to the Executive Head and HR Department for further advice and possible disciplinary action.



INCIDENT CLASSIFICATION AND NOTIFICATION

Incidents will be classified as follows:

Incident Classification	Description	Notification
No Incident	The incident has not jeopardised the confidentiality, availability or integrity of data.	Line manager of the person reporting and any other involved staff.
No Incident – Near Miss	There is a risk that the incident might adversely affect the confidentiality, availability or integrity of data but this has not materialised in this case.	Line manager of the person reporting and any other involved staff.
Low Risk Incident	The confidentiality, availability or integrity of data has been adversely affected however the impact on the Learn to Live Federation and any data subjects involved is negligible.	Line manager of the person reporting and any other involved staff.
Medium Risk Incident	The confidentiality, availability or integrity of data has been significantly affected and there is a measurable impact on the Learn to Live Federation. The incident has not impacted adversely on the rights and freedoms of the data subject.	Line manager of the person reporting and any other involved staff, Executive Head and HR Manager.
High Risk Incident	The confidentiality, availability or integrity of data has been impacted to such an extent that there are significant business continuity risks. The incident has caused a negative effect on the rights and freedoms of the data subject.	Executive Head and relevant Governor.

NOTIFICATION TO THE INFORMATION COMMISSIONER’S OFFICE (ICO)

The ICO will be notified within 72 hours of any incident which might adversely affect the rights and freedoms of a data subject. The ICO interactive reporting tool will be used as part of this assessment.

Notification is the responsibility of the Data Protection Officer following consultation with the Executive Head.



INFORMATION SECURITY INCIDENT INVESTIGATION

The Data Protection Officer will complete an information security investigation and notify relevant staff of the outcome within twenty days of the incident being notified.

Key points are:

- The notification will include a summary of the incident, lessons learnt, action points and relevant guidance.
- If personal data has been inappropriately disclosed, action will be taken to retrieve the data.
- If a member of staff has been negligent, malicious or unreasonable then the HR Manager will decide if further investigation or action is necessary.
- If staff member's actions may constitute an offence under GDPR or the Computer Misuse Act 1990, the matter will be reported to Devon & Cornwall Police.

NOTIFYING DATA SUBJECTS

All incidents which may have a negative impact on the rights and freedoms of data subjects will be notified without undue delay. The notification will include:

- An apology.
- A description of the information put at risk.
- A description of any risk this may cause the data subject.
- A description of how the incident occurred.
- Details of steps taken to remedy the incident and prevent reoccurrence.
- Guidance on how to protect themselves from the effect of the incident.
- Details of how to make a formal complaint to the Learn to Live Federation and the ICO.
- Details of who has been informed of the incident.

The notification will be made in writing.

REVIEW OF INCIDENTS

The Data Protection Officer will ensure that incidents are recorded, monitored and escalated as appropriate.

Actions proposed in response to an incident will be monitored by the Data Protection Officer and reported to Governors on a termly basis.

If actions are not completed or if similar incidents continue, the Data Protection Officer will inform the Executive Head and HR Manager.

RECORD KEEPING

Records of security incidents, investigations and actions will be kept via the CPOMs system.

APPENDIX C TO BE READ IN CONJUNCTION WITH THE DATA PROTECTION POLICY



APPENDIX D

Information Security Assessment

[Name of procurement]

The table below is to be completed by the service seeking to undertake the procurement activity in question. The information provided in this table will help inform the results of the final risk assessment.

1) Name of company
2) Contract reference number
3) Name of contract
4) Contract description
5) Is personal data to be processed as part of this contract
6) If you answered "Yes" to question 5, please describe the processing of personal data which takes place (This should be a high level, short description of what the processing is about i.e. its subject matter)
7) If you answered "Yes" to question 5, please state the duration of this processing (clearly outline any relevant dates).
8) If you answered "Yes" to question 5, please describe the nature of the processing. (The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means)
9) If you answered "Yes" to question 5, please state the type of personal data. (Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc)
10) If you answered "Yes" to question 5, please describe the categories of personal data you process. Examples include: Staff (including volunteers,

agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.

11) If you answered "Yes" to question 5, please outline your plan for return and or destruction of the personal data once the processing is complete. If your contract states you will retain the data please state this. Describe how long the data will be retained for, how it be returned or destroyed.

Devon County Council has a legal requirement to ensure that the personal data we are responsible for is kept secure. To enable us to comply with this requirement, Devon County Council must ensure that any person (whether individually or on behalf of an organisation) processing personal data on the Council's behalf (a data processor) can provide sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and take reasonable steps to ensure compliance with those measures.

Any data processor who has access (directly or indirectly) to personal data held by the Council must complete this questionnaire and where directed, provide evidence showing how they meet the necessary security standards for protecting personal data against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Persons processing data on behalf of the Council which will not have access to personal data (a third party), may still be required to complete this questionnaire if they have access to sensitive business information or business critical systems.

Instructions to data processors and third parties;

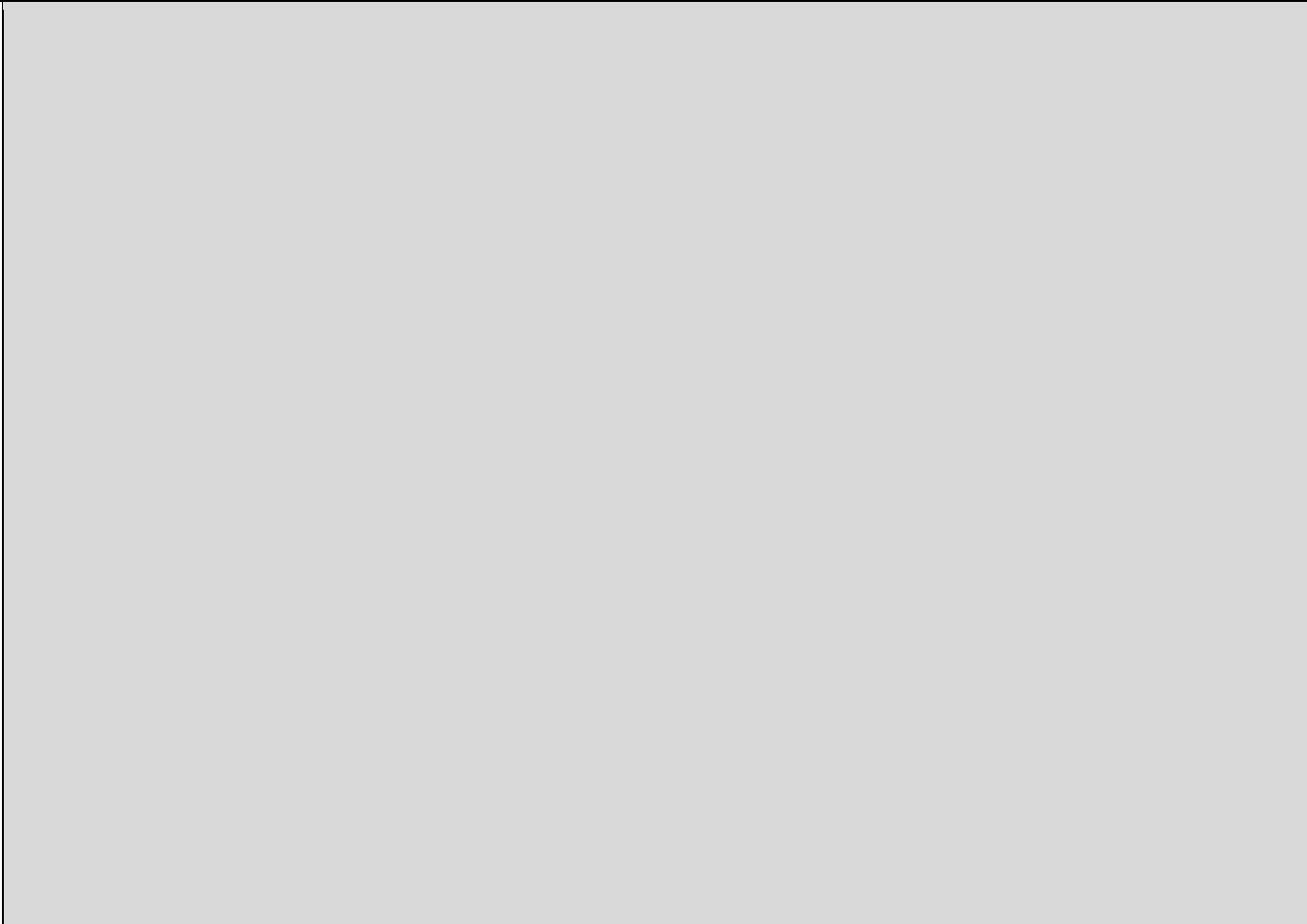
1. This questionnaire must be completed by the individual responsible for Information Security within the company or business tendering for the work being contracted out by Devon County Council.
2. This questionnaire consists of two columns; the first column lists the security questions and the second column requires the data processor or third party to provide their response to the questions. Data Processors and third parties must not modify or delete any questions. If the question does not apply to the services or work that is to be provided, then an "N/A" (not applicable) in the response column is sufficient.
3. Please complete this questionnaire as fully as possible and provide as much information as you are able to. Incomplete or partial answers may result in additional questions and can delay the process. Once the form has been completed, return it to the designated project lead involved in this contract.

- **Name of Bidder:** [bidder name]
- **Evaluated by (IG):** [officer name]
- **Evaluated by (ICT):** [officer name]
- **Outcome:** [Adequate Assurance/ Progressed through Information Risk Assessment]

1.0 General information

Overview of section

Devon County Council requires general information about your company.



1.1 What is the project name?	
1.2 Please describe the project and the work that is being contracted out.	
1.3 What is the name, email address and telephone number of Devon County Council's lead for this project?	

<p>1.4 What is the name and telephone number of your company?</p>	
<p>1.5 What is your company's postal address? If this is different to where the service or work for Devon County Council would be carried out, please include this address also.</p>	
<p>1.6 Does your company own or manage this environment or premises? If not, please identify who does?</p>	
<p>1.7 What is your company's website address?</p>	
<p>1.8 What is the name, email address and telephone number of your company's Information Security or Data Protection Manager or security lead?</p>	

<p>1.9 Is your company registered under the Data Protection Legislation, with the Information Commissioner's Office? If yes, what is your registration number? If no, please explain why not.</p>	
<p>1.10 Is your company certified under the Information Security Standard ISO27001 or accredited to any other security related standard or Code? If yes, please provide details.</p>	
<p>1.11 Describe the type of information or data your company would be processing on behalf of Devon County Council.</p>	
<p>1.12 Will your company be processing personal or sensitive data on behalf of Devon County Council?</p>	

<p>1.13. Will your company be subcontracting any of the work being tendered for? If yes, please provide full details and confirm that authorization has been given by DCC.</p> <p><i>(NB. Subcontracting is prohibited unless Devon County Council has explicitly authorized this. Subcontractors may be required to complete this questionnaire).</i></p>	
<p>2.0 Human Resources Security</p> <p><i>Overview of section</i></p> <p>Devon County Council requires that all individuals who have access to its data are appropriate and trustworthy and are only given access on a strict need to know basis. The Council prohibits the disclosure or distribution of its information to any other third party or data processor, unless explicitly authorized.</p>	

<p>2.1 How many employees does your company have?</p>	
<p>2.2 Please provide details of the background checks your company carries out on new staff or contractors to ensure their reliability and trustworthiness.</p>	
<p>2.3 Please provide a copy of the Data Protection and/or confidentiality clauses included in staff contracts.</p>	
<p>2.4 Please provide details of the information security or data protection training your company provides to its staff. Please include a copy of the training materials.</p>	

<p>2.5 Is information security or data protection training mandatory for your staff and how often is the training provided? If the training is not mandatory for all staff then please explain why not?</p>	
<p>2.6 Please provide details of any incidents involving the loss, misuse or theft of any personal or business sensitive information by your staff in the last 3 years.</p>	
<p>2.7 Has your company self-reported any information security incidents to the Information Commissioner's Office or been reported to the Information Commissioner's Office regarding information security incidents in the last 3 years? If so, please describe the incident(s) and the outcome.</p>	

<p>3.0 Policy and awareness</p> <p><i>Overview of section</i></p> <p>Devon County Council expects your company to have a formal data protection and/or information security Policy, outlining the measures your company takes to protect personal data and or sensitive business data.</p>	
<p>3.1 Please provide a copy of your company policy (or policies) which refers to information security and data protection.</p>	
<p>3.2 Please provide details of how your company promotes awareness of these policies to staff and contractors and any formal training and sign off required.</p>	

<p>3.3 Please provide details of your company’s policy for dealing with Freedom of Information or Subject Access requests that would require the disclosure of Devon County Council data.</p>	
<p>3.4 Please provide details of your company’s policy with regard to Data Retention and Data Destruction.</p>	
<p>4.0 Physical security Overview of section Access to Devon County Council data must be strictly controlled. All data processing devices holding the Council’s data must be held in secure rooms with controlled access. Access to physical media and documentation must also be controlled and must always be held in locked storage when not attended.</p>	

<p>4.1 Describe the physical and electronic security measures used to protect Devon County Council's information on the premises where the information would be held.</p>	
<p>4.2 If the information or data is to be held electronically, where will the data backups be held and what physical and electronic security will be used to secure them?</p>	
<p>4.3 If requested, can a representative from Devon County Council visit the company's facilities to observe the physical security controls in place (announced or unannounced)?</p>	

<p>5.0 Technical controls</p> <p><i>Overview of section</i></p> <p>Devon County Council requires companies and other persons to have appropriate technical measures in place to protect the Council’s personal data and sensitive business data, from unauthorized or unlawful processing and against accidental loss or destruction of or damage to the data.</p>	
<p><i>Segregation of Information between Clients</i></p> <p>5.1 Please provide details of the security controls in place to keep Devon County Council systems and data separate from that held on behalf of your company’s other clients.</p>	

<p><i>Operating System Security</i> 5.2 Please provide details of the Information Security procedures your company uses for protecting its systems against vulnerabilities.</p>	
<p>5.3 Please provide details of the routine vulnerability scanning your company performs of its customer environment and the system tools that are used?</p>	
<p>5.4 What application security test reports for public facing internet-based applications allowing access to Devon County Council data is your company able to provide?</p>	
<p>5.5 What is your company's patch management process?</p>	

<p>5.6 What anti-virus software does your company deploy on its systems and how often are virus definitions updated?</p>	
<p><i>Authentication and Authorization</i> 5.7 Please provide details of the secure encrypted protocols the company uses to manage servers and network devices.</p>	
<p>5.8 What type of authentication is required to access servers and network devices, both from on-site and remote access (e.g. passwords, SecurID)?</p>	
<p>5.9 How is access to the data/information the company would be processing on behalf of the Council controlled? How are duties segregated between staff?</p>	

<p>5.10 Please describe the procedure and system requirements for company's employees to access its network remotely.</p>	
<p><i>Protection of Sensitive Data</i> 5.11 How is electronically held personal data and sensitive business information, protected from unauthorized or unlawful processing?</p>	
<p>5.12 How is electronically held personal data protected against accidental loss, destruction or damage?</p>	
<p>5.14 How will personal or sensitive business data be encrypted both in transit and in storage? Please describe key management practices and the encryption algorithms used.</p>	

<p>5.15 Will your company be holding personal data, belonging to the Council, on its own server or on cloud servers? If yes, is your server or the cloud server held in the European Economic Area? If answering no, please provide details.</p>	
<p>Network Security</p> <p>5.16 Please provide details of the Firewall software that will be used to protect Devon County Council data and systems from the Internet and other untrusted networks, and the formal security accreditations they possess.</p>	
<p>5.17 Please provide details of any intrusion detection/prevention systems used.</p>	
<p>5.18 Please provide details of how frequently security logs are monitored to detect malicious activity.</p>	

<p>5.19 Please provide details of how the company correlates security events from different sources.</p>	
<p>5.20 Please provide details of any wireless technology that will be used and how it will be protected.</p>	
<p>6.0 Organisation standards <i>Overview of section</i> Devon County Council requires companies and other persons to have appropriate standards in place to protect its data. Security incidents must be reported to: KeepDevonsDataSafe@devon.gov.uk These include, but are not limited to, unauthorized access, denial of service, loss or theft of information and data corruption.</p>	

6.1 What is your company's process for disposing of sensitive written or printed material?	
6.2 What is your company's process for disposing of computer equipment used in processing of data?	
6.3 How often are permissions for access to written or printed material and access to computer systems (i.e. physical and logical access) periodically reviewed?	
6.4 What methods would your company employ to verify a user's identity in respect of access to Devon County Council's data (this must include physical and logical access)?	
6.5 What are your company's procedures for reporting security incidents to your clients?	

APPENDIX D TO BE READ IN CONJUNCTION WITH THE DATA PROTECTION POLICY