Third Party User Access Application – External Agencies

v1.1 17 October 2024

Introduction

Worcestershire County Council need to ensure that any access to its data and systems is adequately controlled and accessed on a 'need to know' basis. This is especially important when any access includes personal data and/or special category personal data because we have a duty to ensure that personal data is used and processed properly and in accordance with data protection legislation, including the UK General Data Protection Legislation (UK GDPR) and the Data Protection Act 2018.

By filling in this form you are agreeing to:

- Only access information in the systems on a 'need to know' basis
- Treat all the information you have access to both sensitively and securely
- Be aware that breaches of data will be investigated and may be subject to disciplinary action and
- Be responsible for any loss or claims out of willful improper use of any data
- Comply with the requirements in the Third-Party Organisation Access Agreement.

Which system are you seeking access to?

Name of system / information	
Details / Description	
Purpose for access	

Applicant Details

Full Name	
Organisation Name	
Organisation Address	
Job Title	
Team	
Have you used this system before? Please provide details if you have	

Declaration

Please read the declaration and then sign the request form.

- I understand that information held on our systems should not be used for personal use and in no circumstances disclosed to an unauthorised third party.
- I understand that, I must only use the Liquid Logic systems to obtain information directly linked to my employment. I must not look at any other information. I will not look at details relating to family or friends.
- I understand that it is my responsibility to keep my login credentials secure and only for my own use.
- I understand I need to comply with the UK General Data Protection (UK GDPR) including the Data Protection Principles (see appendix 1 below).
- I understand that access will be monitored by the Council and any abuse of my access will be treated as serious breach of this agreement. Any such breach will lead to access being withdrawn for me and may lead to a review of access provision for other staff in my organisation.
- I understand that it is a criminal offence for me to access and / or process personal data for any other purpose other than that set out in my official duties.
- I understand that, should there be reason to believe that I have breached this agreement, appropriate action may be taken against me
- I understand that if I fail to complete and return this document access to all systems may be removed.

Applicant's Signature	
Date	

WCC Sponsor's Details

Approver's / Sponsor's Name	
Job title	
Date	

Please return the completed form to your Council Sponsor.

The Council Sponsor should then attach the completed form to the relevant catalogue item in MyIT to request an account for the third party. This process will be used to evidence authorisation in lieu of requiring the signature of the Council Sponsor.

Please note, emails or MyIT requests sent directly from the user will NOT be accepted.

Appendix 1 Data Protection Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals (**'lawfulness, fairness and transparency'**)
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**'purpose limitation'**)
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
>
> (d) 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'**)
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (**'storage limitation'**)
>
> (f) 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'**)

Article 5(2) adds that:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**'accountability'**)

Third Party Organisation Access Agreement

Purpose

The purpose of this document is to outline the requirements to support the exchange of personal information between Worcestershire County Council and [insert name of organisation].

Scope

This Agreement describes the responsibilities of Contractors and Third Parties under Data Protection Legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) when:

- undertaking work for or on behalf of the Council, or
- otherwise with the Council which involves accessing the Council's information.

All Contractors and Third Parties who may come into contact with any personal data (as defined in UK GDPR) including any special category data (as defined in UK GDPR), and / or any confidential or sensitive information must follow this Agreement. This includes information held in any format including that held manually or electronically and also information heard during a visit to any Council site.

Definitions

For the purposes of this Agreement the following definitions apply:

Contractor: any company and/or its direct employees who are undertaking work for, on behalf of, or under instruction from the Council. If they are accessing any personal data they likely to be doing so as a Processor under the instruction of the Council and subject to the conditions in Article 28 of the UK GDPR.

Council Sponsor: a Council senior manager who accepts responsibility for the access provided to the Contractor or Third Party

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder)and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended [and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications)[; and the guidance and codes of practice issued by the Information Commissioner or other relevant data protection or supervisory authority and applicable to a party].

Third Party: any person(s) undertaking work with the Council where they are exercising control over the purposes and means of the processing of personal data they are accessing. If they are accessing any personal data they are likely to be doing so as a Controller and are directly responsible for ensuring that any processing of that personal data is in compliance with data protection legislation. If network or system access is required to facilitate any access to personal data, then the information sharing is likely to be systematic and an Information Sharing Agreement is likely to be required.

However, for the avoidance of doubt, any access by Third Parties remains under the supervision, direction and control of the Council, save where expressly agreed with the Third Party.

Controller, Processor, Data Subject, Information Commissioner and **Personal Data, Processing** and appropriate technical and organisational measures shall have the meanings given to them in the Data Protection Legislation

Signatories

All access to the Council's information systems or network must be supported by a Council Sponsor – a senior manager who accepts responsibility for the access provided to the Contractor or Third Party.

A Director or an appropriately nominated senior manager of a Contractor or Third Party can sign this Agreement on behalf of their organisation. The signatory undertakes to ensure that all nominated employees are informed of their responsibilities under this agreement. The Contractor or Third Party must sign the Agreement prior to commencement of:

- undertaking any work using Council data
- any access to Council information and / or systems is provided

All access provided is subject to regular review and re-authorisation from both the Council Sponsor and Nominated Contact from Contractor or Third Party.

Council's Responsibilities

The Council Sponsor is required to obtain a signed copy of this Agreement and send it to the Council's Corporate Information Governance Team (CIGT) to support any access to Council information or systems by the Contractor or Third Party.

The Council Sponsor shall provide to the Contractor or Third Party, the Council ICT and IG Policies (including Data Protection and Information Sharing Policies).

The Council Sponsor must ensure that where Contractors and Third Parties access Council data, they are aware of the appropriate systems, Information Governance and Data Protection training required to be completed by individuals seeking access to Council information or systems.

Contractor and Third-Party responsibilities

They must:

- Ensure that they have read and comply with the Council's Data Protection Policy and all relevant Council ICT and IG Policies
- Ensure that any individual employed or representing the Contractor or Third Party who is seeking access to Council information or systems has completed the relevant system, Information Governance, and Data Protection training, as agreed with the Council Sponsor.
- Be registered under the UK GDPR and the Data Protection (Charges and Information) Regulations 2018 with the Information Commissioner's Office unless exempt, and provide the Council with their registration number when contracted to process Personal Data.
- Ensure compliance with all relevant legislation and ensure the reliability of its employees who have access to any Personal Data
- If required to access or process Personal Data held by the Council, then they shall keep all such information secure at all times (e.g. in a locked cupboard, or encrypted where stored electronically) and shall only process such data in accordance with instructions received from the Council.

- Be aware of the possible impact of the Freedom of Information Act (FOIA) or Environmental Information Regulations (EIR) on information processed on behalf of the Council, including any documentation connected with a contract with the Council.
- If acting as a Processor, at the Council's choice, return all Personal Data to the Council in its entirety or securely destroy / erase all the Personal Data on completion of the task for which the Personal Data was provided or on termination of this Agreement.
- Any transfer method must meet the Council's security requirements including encryption to the required standard.
- Only use and process Personal Data for the purpose for which it has been supplied.
- Any laptop or computer used to process Council information must be encrypted to the approved level; this can be verified with IT & Digital Services.

- Be aware that under Data Protection Legislation a breach of confidentiality may constitute an offence which may lead to a prosecution.

Security

All Contractors and Third Parties connected to the Council's networks must:

- Use the most up-to-date anti-virus / anti-spyware/anti-malware software available
- Be Cyber Essentials Plus certified, or equivalent
- Be protected by a Corporate or private Firewall
- Be up to date with operating system patches
- Not be made available for use to unauthorised third parties
- Be available for inspection by IT & Digital if required.

Related Legislation and Guidance

- EU General Data Protection Regulation and UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Health and Social Care Act 2012
- Confidentiality: NHS Code of Practice 2003
- Caldicott Principles and the Common Law Duty of Confidentiality

Organisation Signatory Details

Name of Organisation	
Name of Signatory	
Signature	
Date	

WCC Sponsor's Details

Approver's / Sponsor's Name	

Job title	
Date	