Data Protection Impact Assessment (DPIA)

Project Name:	End User Device (Laptop) Upgrade + tablets and desktop PCs
Project Manager or Sponsor (PM):	Mark Line
Name of person completing the DPIA if different to (PM):	
Service Team and Department:	CDS / ACE
Relevant Director and Executive Director:	Paul Golland / Elaine Jackson
Cost Code:	800240
Date DPIA received by the IMT:	24/05/2023
Date advise finalised by DPO:	
Date approved by IMT :	

The laptops currently in use across the council are rapidly becoming obsolete, and no longer supported by the manufacturer. The device specifications are also no longer fit for purpose to meet the hybrid working model operating across the council.

The purpose of this project is to replace circa 3700 devices for all existing employees taking back their current device and providing a new replacement, this is to happen over a 6 month to 9 month period, with a rolling provision of devices to new starters as well as staff requiring a replacement device over a 4 year contract period.
New technology will also be implemented to streamline and speed up the set-up of user account profiles, install and patch application software and improve management of devices in general.

This DPIA covers 3 areas of the upgrade, the asset registering of equipment to the employee, the optional use by them of the 'Biometric log on' functionality, and the optional home delivery service.

1 Project Scope:

2 Data Description

Answer the questions below so that there is a clear understanding about how the information will be used, who will use it etc. Remember that it's personal information (i.e. information about individuals) that you need to be concerned with. If you do not have answers to all the questions at this time, simply record what you do know.

- Whose information is being used? *Are there additional concerns that need to be considered due to individuals sensitive/*	**Asset Tagging** Employee data as all LBC employees who will be issued with a new LBC Laptop

complex circumstances? i.e. vulnerable person	device.(also desktop PCs and Tablets are in scope, but on a case by case basis). **Biometric log on** Also the optional use by an employee of a 'Biometric log on', will be made available as part of this project. **Home Delivery** Also a preferred but optional delivery method to an employee's home address
What information is being used? - *Consider the nature of this information E.g. Child's social care file*	Employee's will be required to accept a Privacy Notice which will explain any personal data captured and how it will be used. The Staff Data Protection policy will also be reviewed to make sure it is up to date where appropriate for the following 3 areas. **Asset Tagging** Each user will have their name logged against the specific device via the Asset tag. This data will be stored on the main IT Configuration Management Database (CMDB) which is managed by LittleFish as per the current LBC IT Service Delivery contract. **Biometric log on** Microsoft have developed the "Windows Hello" system that enables users to use biometric data to authenticate when logging on to a device. This is normally done by scanning a fingerprint, or facial recognition which is then converted into a digitised template. **Home Delivery** Each user receiving a new laptop has our preferred option of having the device delivered to their home address by courier, this will require the staff member to provide

	their address and a contact phone number when booking a delivery slot.
Does it include special category or criminal offence data?	**Asset Tagging** No **Biometric Log on** The use of Biometric Data as part of the log on process is in of itself Special Category Data. **Home Delivery** No
Can an individual be identified easily from the information?	**Asset Tagging** Yes. The Laptop's asset tag/no will be logged against an individual member of staff, as being issued to them. This will be held in CMDB and will consist of first name, surname, employee number and LBC email address logged against their specific device. No other personal data is stored within the CMDB. **Biometric Log on** If the option of a Biometric log on is chosen by an employee, that information will be only stored on the device to which it relates. **Home Delivery** Yes. The employee will be asked to provide their Name, Address and contact phone number. Until the tender responses are received, and the contract awarded it is not yet clear where this data will be held and managed. This DPIA will be updated once the information is available.
What is the potential impact on privacy of this information? - *What are the risks/ impact to an individual if this information was lost, stolen or manipulated?*	**Asset Tagging** Little or none. No one other than designated CDS and Littlefish staff can access the CMDB and this information is in effect business information, which relates

- *E.g. could it be sold?*	to the issue of an asset to an employee. Apart from the Service Delivery Team, access to the CMDB by CDS staff must be requested from LittleFish. **Biometric Log on** Any Biometric log on data cannot be accessed; the digitised biometric data is stored on the laptop only. It doesn't roam and is never sent to other external devices or servers. **Home Delivery** If the information was lost or stolen, then there is the potential for an employee to receive unsolicited phone calls and post.
Will this change the manner in which we handle, use or protect this information? *e.g. should it be encrypted?*	**Asset Tagging** No. The Data held in the CMDB is protected by the Council's IT Security systems, and access is strictly controlled **Biometric Log on** No. Like the current laptops the new laptops will be hardware encrypted. **Home Delivery** It is expected that a 3rd party bookings portal supplied and managed by the contracted supplier will capture and hold the employee data and until the tender responses are received and the contract awarded we do not know the details of system that will be used. As part of our technical specification for the tender we will be asking for full details of what solution the supplier would be using and asking that it meets the Council's data protection requirements. LBC Data Protection requirements will be part of the Tender Specification and will include: - Data Security and due diligence review of the contractor's processes; - A Data Sharing Agreement to

	include restriction on the retention of staff data and secure disposal of the that data to be part of the Contractual Terms (including penalties for misuse of that data) - No data to be stored outside of the UK. This DPIA will be updated once the information is available.

3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	**Asset Tagging** Not required **Biometric Log on** August 2022 with target group of end users and LBC Disability Forum. See further details below. **Home Delivery** April 2023 with project board members and key stake holders.
How did you consult individuals?	**Asset Tagging** No consultancy was required. **Biometric Log on** We have carried out some top-level end user requirements gathering with a target group of end users (circa 160 staff), and the LBC Disability Forum to identify the requirements that will help build the overall requirements that will be used for the procurement process. Biometric Authentication has been identified as a user requirement from some respondents. It has also been specified to be included in the device build by the CDS Technical Architects.

	This was done by emailing an MS Forms based questionnaire: https://forms.office.com/r/Wf9t0pL3FY HR are to be made aware of this optional device login for employees and they will be asked to inform trade unions if they feel it appropriate. **Home Delivery** End users have not been consulted. Workshops with project board members and key stake holders have been held to outline and agree project scope, it has been agreed that a home delivery service option needs to be provided to give flexibility and user satisfaction. HR are to be made aware of this optional service for employees for this specific project and they will be asked to inform trade unions if they feel it appropriate.
If not explain why it is not appropriate.	**Asset Tagging** Asset tagging is a mandatory security requirement for managing the Councils assets. The Council's IT Security Policy will be reviewed and if this is not already specifically covered it will be added. **Home Delivery** End users were not consulted as this will be an option and has been identified as a requirement for the project scope by key stake holders.
Who else within the organisation have you consulted with?	IM / Legal and CDS Technical Architects
Do you need to speak with your processor to assist?	No - the Council is the Data Controller/Processor
Do you plan to consult information security experts or any other experts?	LBC Digital Security Manager have provided their feedback to this DPIA.

4 Assessment of necessity and proportionality of data usage

What is your lawful basis for processing?	**Asset Tagging** The Council has a Legitimate Interests under Article 6 (f) to process the employee data as it is necessary to meet the Council's legitimate interests in controlling the use of assets provided to employees for the purposes of work. The use of the employee data that is processed under Article 6 (f) relates only to the use of employee data to log and maintain the CMDB records of who has which device for asset management purposes. **Biometric Log on** The optional use of a Biometric Log on by an employee would be based on Consent (Article 6 (a)) and as this amounts to the use of Special Category Data, also Article 9 (a) again based on explicit Consent. **Home Delivery** This will be an optional service and for the service to be provided the employees Name, Address and Contact phone number will be required.
s consent being relied upon to share the nformation? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?	**Asset Tagging** No - For the purposes of the allocation of Council assets, the Council is exercising a legitimate interest in identifying users an asset is allocated to. **Biometric Log on** Yes - Any use of a Biometric Log On is entirely optional, and a choice exercised by the employee. **Home Delivery** Yes - A home delivery will be entirely optional (office collection alternative will be available) and the employee will be asked to provide consent.

Does the processing actually achieve your purpose?	Yes
How will the information be collected? (Verbally, forms, intranet, interview, 3rd party, anonymous)	**Asset Tagging** A log of the laptop Asset Tag number allocated to each employee will be made to update and maintain the CMDB **Biometric Log on** The laptop device captures, encrypts and holds the data locally; the digitised biometric data is stored on the laptop only. It doesn't roam and is never sent to other external devices or servers **Home Delivery** It is expected that a 3rd party bookings portal supplied and managed by the contracted supplier will capture and hold the employee data and until the tender responses are received and the contract awarded we do not know the details of system that will be used. As part of our technical specification for the tender we will be asking for full details of what solution the supplier would be using and asking that it meets the Council's data protection requirements. This DPIA will be updated once the information is available.
Is there another way to achieve the same outcome?	**Asset Tagging** No **Biometric Log on** This is an optional choice for the employee and other standard log on methods can be used. **Home Delivery** This is an optional choice for the employee, the alternative is for the employee to collect the laptop from LBC offices.
How will the information be used? *e.g. to write a report*	**Asset Tagging** Information held within the CMDB will record the allocation of specific devices to

	each employee. **Biometric Log on** The employee's laptop will use the data to verify them as a legitimate user for the laptop and provide access. **Home Delivery** The information will be used to facilitate the delivery of a new laptop direct to the employee from a 3rd party contractor. Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. This DPIA will be updated once the information is available.
Do the individuals know and understand how their information will be used? If there are changes to their information does the privacy notice need to be amended?	**Asset Tagging** It would seem to be a reasonable expectation that a record would be retained of an asset issued to them. **Biometric Log on** Employees will be provided with information which will include a Privacy Notice and information on the optional use of Biometric Log on, should they choose to use that option. **Home Delivery** It would seem to be a reasonable expectation that address and contact details will be required for this service to be provided. Employees will be provided a Privacy Notice and information on the optional home delivery service and employee consent will be required.
How will it be stored, kept up to date and disposed of when no longer required? *e.g. stored in locked cabinet/securely shredded*	**Asset Tagging** Any user data will be updated / removed from the CMDB as part of the Leaver process and once the asset has been returned. **Biometric Log on**

	All data stored on the device which will include any Biometric data will be wiped and lost when a Laptop is returned and either re-built ready for re-issue or wiped and disposed of. **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. Suppliers will be asked to provide details of how the data will be held and disposed of following completion of a delivery request. LBC Data Protection requirements will be part of the Tender Specification. The final agreed process will be recorded in an updated version of this DPIA, which will be used to control the delivery of Laptops to those staff who request this option
How will you ensure data quality and data minimisation?	**Asset Tagging** The only data required will be the End Users' Name and Employee Number, which forms part of the Sign-in User-ID. **Biometric Log on** N/A **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. It is fully expected that only the Employee's name, Address and Contact phone number will be required, and the employee will be asked to provide this information. The final agreed process will be recorded in an updated version of this DPIA.
Who will have access to the information within LBC? - *Include approximate number of users*	**Asset Tagging** CDS staff – 6-10 employees (mainly Service Delivery Management, Business

	Analysts & Technical Architects on an ad-hoc basis. **Biometric Log on** There will be no access to any Biometric data which is stored in a secure and encrypted format on a Laptop. **Home Delivery** It is expected some CDS staff working as part of the project delivery team will require access to this information to help manage and trouble shoot any delivery issues.
Are there new or significant changes to the way we manage, use, handle or collect this information? - *Include any identified concerns for the individuals, would these changes heighten risks involved*	No
Will individuals within an existing database be subject to new or changed handling? - *If yes amendments need to be made to the privacy notice and these individuals need to be informed.*	No
What are the internal arrangements for processing this information? *e.g. number of staff who will have access*	**Asset Tagging** The CMDB is maintained by LittleFish as part of the Asset Management Process. CDS Service Delivery, Technical & Analyst resources may require access for reporting and project work. If LittleFish respond to this tender, either directly or via a partner and are awarded the contract, they will be required to keep their BAU activities separate to any contract related activities involving employee data to prevent any breaches of DPA. **Biometric Log on** There will be no access to any Biometric data which is stored in a secure and encrypted format on a Laptop. **Home Delivery** It is expected that only a couple of CDS project management, business analyst,

	and project administration staff working on the project delivery will require access to this information to assist in resolving any delivery issues. It is expected that they will have direct access to the information held on the 3rd party supplier's system. Employee home address information currently held within corporate systems and typically used by HR staff will not be used for any address verification and there will be no requirement for HR to be involved with this specific address data.
How will the information be updated? *e.g. monthly check*	**Asset Tagging** As and when users leave or join the council or require a replacement device issuing to them. A separate requirement outside of this project is to review the starters and leavers policy with HR to help address the poor return rate of laptops from leavers. **Biometric Log on** Only when an employee chooses to initially set-up a biometric log on or if they need to reset/update the log on. **Home Delivery** This will only need to be done once when the employee first decided to use this service.
Does the project involve the exchange of information outside of the UK and are there set standards for how the information will be treated? How will you safeguard international transfers?	No – Although we will not know the exact process until the contract is awarded it will be a tender specification requirement that data cannot be held outside of the UK.
How will you prevent function creep?	The project scope specifically deals with the procurement and deployment of new end user laptops, tablets and desktop PCs for the Council staff. No other user groups, or devices are included within this project.

5 Assessment of the risks to the rights and freedoms of data subjects

You must describe the source of risk and the nature of potential impact upon individuals and identify any additional measures to mitigate those risks.

5a Security

Who will be responsible for the control for this information?	Paul Golland - Interim Chief Digital Officer & Director of Resident Access. Jon Raby - LBC Service Delivery Manager
How will the access to this information be controlled?	As per current LBC data protection and Security processes and procedures.
Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?	**Asset Tagging** Yes, the CMDB is maintained by LittleFish as part of the Asset Management Process. CDS Service Delivery. **Biometric Log on** The optional use of a Biometric Log On by employees provides increased security and an improved user experience when logging on to the device. Should a user leave, this information will be deleted as part of the device re-build prior to being re-issued to another user, or as part of the device wipe before being retired. A Biometric Data Security policy exists (this forms part of this DPIA) to address the Biometric Functionality. This will be revisited and updated as necessary and once approved, will be published as part of ICT Data and Security policy (this also forms part of this DPIA). **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. The tender specification will request full details of how employee's data will be managed and secured.
Are there adequate provisions in place to protect the information? If so what are they? *e.g. Process, security*	**Asset Tagging** The CMDB is maintained by LittleFish as part of the Asset Management Process. CDS Service Delivery. Only the employee's name and LBC employee ID is held against an asset.

	Data is removed if the employee leaves. **Biometric Log on** In respect of the optional use of Biometric Log On, the digitised biometric data is stored on the laptop only. It doesn't roam and is never sent to other external devices or servers. This separation helps to stop potential attackers by providing no single collection point that an attacker could potentially compromise to steal biometric data. In the unlikely event that an attacker was actually able to get the biometric data from a device, it cannot be converted back into a raw biometric sample that could be recognised by the biometric sensor. **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. The tender specification will request full details of how employee's data will be managed and secured.

5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	**Asset Tagging** Device (Asset) Management is managed by LittleFish as per the current IT contract in place with them. **Biometric Log on** Not shared **Home Delivery** The awarded supplier for this contract will be required to capture this information to provide the delivery service, until the tender responses are received and the contract awarded we do not know who the supplier will be. It is also reasonable to assume the supplier

	will use a courier to provide the delivery service and the courier will also require the name and address details.
What purpose does the information we are sharing have to the third party? - *Ensure that we only share relevant information and not excessively*	**Asset Tagging** To allow Littlefish to manage end user IT support and management of IT assets. **Biometric Log on** Not shared **Home Delivery** The employee's name and address details are required by the supplier to manage the home delivery service and it is required by any courier engaged with by the supplier to provide the delivery service.
Who will have access to the information, externally? - *Include approximate number of users* - *Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.*	**Asset Tagging** LittleFish – 10-15 (Service Delivery Management, Project Managers and Deskside Support staff) **Biometric Log on** Not access externally; the digitised biometric data is stored on the laptop only. It doesn't roam and is never sent to other external devices or server **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place. This DPIA will be updated once the contract is awarded and the information available.
How will it be transmitted to third parties and when? How often? - *Provide details of software used*	**Asset Tagging** Littlefish have access to the CMDB as part of their Service Delivery. **Biometric Log on** No third party will have access to the Biometric Log On data. **Home Delivery** Until the tender responses are received and the contract awarded we do not know the

	details of the delivery service and process that will be put in place. It is envisaged that the supplier will have a bookings portal where employees book a delivery appointment, this should only need to be done once but an employee may want to change a booking. This DPIA will be updated once the contract is awarded and the information available.
Is there a data sharing agreement in place?	**Asset Tagging** Yes- this is included within the main Service Contract we have with LittleFish. **Biometric Log on** No third party will have access to the Biometric Log On data. **Home Delivery** Until the tender responses are received and the contract awarded we do not know the details of the delivery service and process that will be put in place.
At what stage will the information be transferred?	**Asset Tagging** Once the deployment phase of the project begins, and then on an ongoing basis when change of laptop "owner" arises **Biometric Log on** No third party will have access to the Biometric Log On data. **Home Delivery** Once the deployment phase of the project begins, and then on an ongoing basis when a new starter requires a laptop via home delivery, or an existing employee needs a replacement laptop via home delivery.

5c Identified Risks and assessment:

You should take into account the sensitivity of the information and potential harm that inappropriate disclosure or use of the information could cause to any individuals concerned. You should also consider the reputational loss to the Council and the potential for financial penalties being imposed by the ICO.

To assess the level of risk you must consider both the **likelihood** and the **severity** of any impact on individuals. A high risk could result from either a high probability of some harm or a lower possibility of serious harm.

The severity impact level and likelihood should be scored on a scale of 1 to 10 with 1 being low severity and 10 high. The two scores should be **added** together. The RAG status is derived from the following scale:

Score:

- 15 to 20 = Red (High)
- 8 to 14 = Amber (Medium)
- Below 8 = Green (Low)

To be completed by Project Sponsor

Risk Identified	Severity of Impact	Likelihood of harm	Overall RAG rating
LBC user can be identified via device Asset Tag	1	1	1
Incorrect assignment of user to asset tag	1	1	1
Accidental omission of user or asset from the CMDB	1	1	1
Loss or corruption of asset data in the CMDB	1	1	1
Unauthorised access to CMDB asset tagging data	1	1	1
Employee name, address and contact phone number unlawfully obtained from suppliers booking system by 3rd party	3	2	5
An employee's address or phone number is accidently shared with a different employee.	2	1	3
Laptop delivery is accidently delivered to wrong address revealing employee name and address	2	1	3

6 Identify measures put in place to reduce risk.

You must now identify additional measures you could take to reduce or eliminate any risk identified as medium or high risk in step 5.

To be completed by the Project Sponsor

Risk Identified	**Options to reduce or eliminate risk**	**Effect on risk** *Eliminated / reduced / accepted*	**Residual risk** *Low / medium / high*	**Measure approved** *Yes / No*

Sign off and Record sheet

Item	Notes, **Name and date**
Measures approved by:	
Residual risks approved by: *(If accepting any residual high risk must consult ICO before going ahead.)*	
IM advice provided:	
Having met with CDS and discussed their processing requirements the following advice has been provided in addition to revisions in the description of processing with the body of the DPIA: **Biometric Log On** - this is an option that may be exercised by an employee. To enable them to exercise the appropriate level of 'consent' they should be provided with a **Privacy Notice** setting out how their data will be processed on the laptop as well as a **Security Notice** setting out how their data is secured on the laptop. **Configuration Management Database** - again all employees should be provided with a Privacy Notice setting out how their data will be stored and processed. **Record of Processing Activity (RoPA)** - the Configuration Management Database could be used as RoPA, to capture the processing of the employee data and the assets issued to them. **Data Controller** - from the description of the processing the Council would appear to be the Controller and Littlefish the Processer in respect of the data held on the Configuration Management Database. **Staff Data Protection Policy** - CDS should liaise with the People Service, to consider whether the Staff Data Protection Policy requires any revision in respect of the processing that is set out within this DPIA. **Security and Biometric Security Policies** - these should form part of this DPIA, once they have been revised. Again, the Staff Data Protection policy should be reviewed to take into account any relevant revisions that may be required to account for the use of employee Biometric data. **Home Delivery** - is being considered as an option for those staff who do not wish to collect their new Laptop from BWH. It is understood that this will be offered as an	

option and only those staff who choose this option will receive a 'home delivery'. This will require safeguards to protect the data. These points should be included within the Tender Specification:

- Data Security and due diligence review of the contractor's processes;
- A Data Sharing Agreement to include restriction on the retention of staff data and secure disposal of the that data to be part of the Contractual Terms (including penalties for misuse of that data);
- The Home Delivery Data should not be held any longer than strictly necessary, (perhaps 2 months after last action) for the purposes of audit and managing any 'snagging issues', following which it should be securely disposed of and Certificate of Destruction issued by the Contactor
- No data to be stored outside of the UK.

Further there should be no 'linking' of the data provided by staff to any other data held by the Council.

IM sign off:	
DPO final sign off:	