Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

For assistance or to submit a DPIA for approval email IGhelp@ico.org.uk.

You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions

Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	
Project Title:	Windows Hello
Project Manager:	Deborah Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme is currently an invite only programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft 365 E5
    - Office 365 E5
    - Windows 10 Enterprise E5
    - Enterprise Mobility + Security E5
- Microsoft Managed Desktop IT as a Service
    - Microsoft Support (“Get Help”)
    - Microsoft Operations & Monitoring
- A Microsoft Surface Device

DPSIA’s have already been completed for the following areas;

- Office 365 including Enterprise Mobility + Security
- Microsoft Get Help 24x7 Support (“Get Help”)
- Microsoft Windows Diagnostics and Telemetry (Advanced Threat Protection)

Additional DPSIA’s will be completed for;

- Microsoft Cortana Voice Recognition
- Get Help
- MMD threat protection

Scope of this DPIA

- Windows Hello Biometric Framework

Windows Hello is the Microsoft Window’s biometric login framework, its purpose is to provide a replacement for password based login, using your face (or on some devices, fingerprint), authentication certificates and certificates stored on the Microsoft Surface device to log you into your device, software and network resources.

Windows Hello is a faster way of logging into your device and reduces the risk associated with compromised passwords.

When you first register with Windows Hello on your new Surface device, the webcam array uses your facial geometry to create a data representation of your face, this isn’t a photograph but an encrypted graph based on the distances and depths of your facial features. This encrypted graph is stored on your device only.

When you log into your device, your facial geometry is used to unlock a user authentication certificate stored in the device’s TPM chip (a secure enclave on your device’s motherboard), which is used to unlock your device and authenticate you to your resources.

The data representation of your face is encrypted and stored on your Surface device only, it is not sent to Microsoft or stored anywhere else, it cannot be exported from the device and is used only for the purposes of user authentication by the Windows Hello framework. Applications may talk to the Windows Hello framework to verify your identity but the framework will only respond with pass or fail for the authentication attempt.

Users have the option of falling back to PIN based authentication if they do not wish to enrol in the biometric framework, the encrypted PIN is stored on the device and is subject to same complexity requirements as the ICO’s user login password.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a “record of processing activities” for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Microsoft
Purpose of processing	Biometric User Authentication
Categories of data	Biometric graph of facial features, user telephone number.
Categories of subjects	ICO Staff
Categories of recipients	Microsoft – only the telephone number for the purpose of multi factor identification.
Overseas transfers	To Microsoft in the USA. Microsoft have a current Privacy Shield certification.

1.4 Purpose for processing

Guidance: State the business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

Windows Hello Biometrics are used to improve the security posture of the ICO by reducing the need for passwords which are often regarded as a weak point in user authentication.

The user is briefed on Windows Hello as part of on-boarding process. If a user does not wish to enrol in the biometric elements of Windows Hello, then they are free to use PIN authentication only.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

The lawful basis for processing is Article 6(1)(a) – consent. The basis for processing special category data is Article 9(2)(a) – explicit consent.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy
a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

Retention & Deletion
d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period

f) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>

g) The data subjects shall be provided with:

(i) The identity and contact details of the data controller;

(ii) The purposes of the processing, including the legal basis and legitimate interests pursued

(iii) Details of the categories of personal data collected

(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>

h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject

i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely

k) Identify an Information Asset Owner

l) Update the Information Asset Register

<u>Is the data being transferred outside the UK and EEA? If so:</u>

m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries

n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>

o) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>

p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject

q) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>

r) *Update the Privacy Notice*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, “Internet of Things” applications can have significant impacts on subjects’ daily lives and privacy. Note: Screening question not considered to be met. Whilst	N

	facial geometry login for electronic devices is new to the ICO this is not a recent or new technological development in the world at large.	
9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Consultation will take place with the DPO Team / Cyber Security as part of completing this DPIA. There has been some consultation with end users during the proof of concept stage to understand their general views about use of this technology at the ICO. End users are given an explanation and a choice during the MMD onboarding as to whether they wish to consent. Use of biometric user authentication is entirely optional.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*

- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

The graph of facial features and the users telephone number are collected directly from the data subject as part of the MMD onboarding process, after the project team have explained the functionality to the user and obtained their explicit consent.

End users are asked:

Based on the information above:

□ **I agree** to the use of Windows Hello on the understanding that the image created is only held on the device provided to me and is not stored elsewhere and also that it is not used for any other purpose other than for accessing my device.

□ **I do not** wish to use Windows Hello at this time

Name:

Signed ……………………………………………………………………..

Date ……………………………

The biometric graph is encypted using strong cryptography and stored on the device only, this graph is only accessible through the Windows Hello framework which will return 'pass' or 'fail' for the authentication attempt. The biometric data is not accessible outside of this framework, it cannot be exported, uploaded or transferred.

User Biometric Graph can be updated by a user as required, after failed biometric login attempts, user is prompted to update biometric graph to improve accuracy.

The users telephone number is obtained and is provided to Microsoft for the sole purposes of user verification as part of multi-factor authentication (an enhanced security feature used as part of the PIN reset process).

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	**Recipients**	**Retention Period**	**Necessity**
Encrypted graph of facial geometry	None – stored on device only	The facial geometry graph is updated when manually triggered by a user (“Improve Windows Hello Recognition”). Otherwise the facial geometry graph remains encrypted on the device until the user profile is removed or the device reaches the end of its usable life. Data can be wiped from the device by a factory reset by ICO IT staff	This is required for the Windows Hello Biometric framework to support facial login to Microsoft Surface Devices.
Telephone number	Microsoft	Held by Microsoft for the period the user requires access to the device. The user device data is deleted 90 days after ICO leaver process concluded. We can add legal holds and request Microsoft retain user data for longer periods if required.	Necessary for security of the device and the multi factor identification.

4. Compliance measures

Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	User can update information if significant change to facial geometry occurs. The user is prompted to update this in the event that sign in fails to improve accuracy of logins. User can update multi factor authentication from Microsoft security portal in Office 365.
b) There must be means to validate the accuracy of any personal data collected	Success or failure of the login process will validate the collection of the data and the user can update when necessary as detailed above.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	User can update the information as required.
Retention & Deletion	
d) All data collected will have a retention period	Data is retained for the duration of the devices assignment to a user or until the device reaches the end of it's usable life ICO IT will carry out reset of device before any assignment to a new user or at end of life.
e) Data must be deleted at the end of its retention period	Data is stored on the device and is destroyed when the device is reset or the user profile is removed.
f) Personal data must be erased upon receipt of a lawful request from the data subject	User can be unenrolled from Windows Hello Facial Recognition but will require a device rebuild.
Information & Transparency	
g) The data subjects shall be provided with: • the identity and contact details of the data controller; • the contact details of the Data Protection Officer; • the purposes of the processing, including the legal basis and legitimate interests pursued • details of the categories of personal data collected • details of the recipients of personal data	Information is provided to users during the device onboarding process and consent to the processing of biometric data is obtained from the user.
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	User can opt out of Windows Hello facial recognition process
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	User can opt out of Windows Hello facial recognition process
Security	

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Information is provided to users during the device onboarding process, ICO staff are available during on-boarding to support the process. Microsoft Windows has detailed instructions to support the user during the process.
k) Identify an Information Asset Owner	Director of Digital, IT and Customer Services.
l) Update the Information Asset Register	Updated by Information Management and Compliance.
Conditional Requirements	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Data is not transferred, it does not leave the user's device.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	DPO consulted as part of DPIA process.
o) There must be controls to ensure or monitor compliance by external organisations.	N/A
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A.
q) The consent must be recorded in some manner to serve as evidence	Users sign consent declaration during the MMD onboarding process. Consent records are retained by the project team.
r) Update the Privacy Notice	Staff privacy notice to be updated to include information about MMD devices.

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Device allows access to unauthorised third party due to false positive	*High – user device and documents are accessed*	*Very low – Less than 0.001% chance of occurrence.*	*Risk level Low and is accepted.*
Device may not process biometric details correctly and blocks access to the authorised user.	Low - User will be denied access to the device and will be prompted for a PIN in the first instance or an automated phone call to a number set at enrolment if a user cannot remember their PIN	Low – processing of facial biometric data is affected by lighting conditions and presence of glasses etc however in the event of failed login user has alternative means of access via pin	*Risk level Low and is accepted.*
Data Accuracy & Sufficiency	Low - User can update biometric	Low – User can improve data	*Risk level Low and is accepted.*

	data at any time and is prompted to do so in the event of a login failure.	accuracy at any time	
Illegitimate Access to Data – A rogue application or actor may be able to access and decrypt the biometric data stored on the device. This could potentially result in a recreation of a users face.		Very Low – MMD security layer prevents non-ICO approved applications from being installed on the device and identifies 'unusual' user behaviour. There are no known methods of achieving this outcome. There are no known methods of reversing the encryption without key.	
Unauthorised / Incorrect Modification – A rogue application or actor may be able to access, decrypt and modify the biometric data stored on the device.	High – *user device and documents are accessed*	Very Low – MMD security layer prevents non-ICO approved applications from being installed on the device and identifies 'unusual' user behaviour. There are no known methods of achieving this outcome. There are no known methods of reversing the encryption without key.	*Risk level Low and is accepted.*
Destruction or Loss of Data - The biometric data stored on the device may be lost or destroyed.	Low – User will be denied access to the device and will be prompted for a PIN in the first instance or an automated phone	Low – In the event of device loss, data is inaccessible due to encryption. ICO policies are to initiate a remote	*Risk level Low and is accepted.*

	call to a number set at enrolment if a user cannot remember their PIN	wipe on lost devices which would reset the device to factory fresh status.	

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	**Recommendation**	**Project Team Response**
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Considered by	**Date**	**Project Stage**
DPIA Forum	20/02/2020	

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
v.0.1	07/02/2020	Neil Smithies	First Draft

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.1
Status	Final release
Owner	DPSIA Committee
Release date	02/04/19
Review date	10/12/20

Appendix: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix A – Windows Hello information & agreement provided to end users

Stay relevant, provide excellent public service and keep abreast of evolving technology.
GOAL 4
BUS

'Maintaining and increasing our technical understanding of the environment we regulate goes hand in hand with our own use of technology in our services and working practices as we continue to invest in technology and skills the public would expect of a modern regulator.'

As part of your new device roll-out we are offering you the option to use Windows Hello facial recognition authentication as a quick, modern and more secure way to access your device. For this reason it is the ICO's preferred authentication method.

However, the use of Hello is not required for your device to work, you will have the option to log in using two factor authentication such as PIN and password. This will not restrict functionality, but will require you to log in to your applications each time.

We understand that you may have some questions about the use of biometric data, so the following information is intended to explain what happens when you use Windows Hello, and enable you to make an informed decision about whether you want to activate this.

In order to ensure we are GDPR compliant we will ask you to indicate your decision below, and this information will be retained to record your consent.

Should you change your mind you may remove this functionality yourself in a few simple steps, and can retract your consent at any time by emailing ithelp@ico.org.uk

Windows Hello, Biometrics and Privacy.

Windows Hello is the Microsoft Window's biometric login framework, its purpose is to provide a replacement for password based login, using your face, authentication certificates and your new device to log you into your device, software and network resources.

Windows Hello is a faster way of logging into your device and reduces the risk associated with compromised passwords.

When you first register with Windows Hello on your new Surface device, the webcam array uses your facial geometry to create a data representation of your face, this isn't a photograph but an encrypted graph based on the distances and depths of your facial features. This encrypted graph is stored on your device only.

When you log into your device, your facial geometry is used to unlock a user authentication certificate stored in the device's TPM chip (a secure enclave on your device's motherboard), which is used to unlock your device and authenticate you to your resources.

The data representation of your face is encrypted and stored on your Surface device only, it is not sent to Microsoft or stored anywhere else, it cannot be exported from the device and is used only for the purposes of user authentication by the Windows Hello framework. Applications may talk to the Windows Hello framework to verify your identity but the framework will only respond with pass or fail for the authentication attempt.

For more info, please refer to the following resources on the Microsoft site:

https://support.microsoft.com/en-gb/help/4468253/windows-hello-and-privacy-microsoft-privacy

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

https://docs.microsoft.com/en-gb/windows-hardware/design/device-experiences/windows-hello-face-authentication

Based on the information above:

□ **I agree** to the use of Windows Hello on the understanding that the image created is only held on the device provided to me and is not stored elsewhere and also that it is not used for any other purpose other than for accessing my device.

□ **I do not** wish to use Windows Hello at this time

Name:

Signed ……………………………………………………………………..

Date ……………………………