Privacy Statement on the processing of personal data in MS Teams (collaboration application of Office 365)

What is the nature and the purpose(s) of the processing operation?

Since the outbreak of the coronavirus COVID-19 virus, the Council has extended the use of Microsoft Office 365, and in particular 'Microsoft Teams' to organise virtual meetings and teleconferences with internal staff and external stakeholders. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. The personal data is collected and stored in Harrow Council's Microsoft Cloud servers with the purpose of providing the above-mentioned services. The processing is not intended to be used for any automated decision making, including profiling.

The protection of your privacy is of the utmost importance to Harrow Council. We are committed to respecting and protecting your personal data and ensuring your rights as a data subject. All data of a personal nature, namely data that can identify you directly or indirectly, will be handled fairly, lawfully and with due care. We have applied appropriate technical and organisational tools and structures to comply with the GDPR.

What personal data do we process?

The categories/types of personal data processed are the following:

Personally identifying Information: username, name, surname, email, work Telephone number, current function and preferred language. (either entered personally by you when you access Microsoft Teams, or applied by your workplace when your account is created)

Electronic identifying information: IP address, cookies, connection data and access times.

Movies, pictures, video and sound recordings: all recordings are to be made under consent by all parties in the meeting, consent and reference to this privacy notice should be agreed before recording has taken place. Members of the public, councillors and staff joining democratic meetings should note that as part of our modernisation and governance procedures, Harrow video record all meetings and upload these to youtube.com as a record of the content. Attending these meetings is based on consent as it would be for those attending an office-based meeting. If the attendee does not want to consent to the video recording, other methods such as written, pre-recorded submissions should be allowed or a substitute attending on behalf.

Metadata used for the maintenance of the service provided.

Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar)

Who is responsible for processing the data?

The processing of personal data is carried out under the responsibility of the Information Technology team. The IT team use the data supplied for access to and within Microsoft Teams to:

- Provision end-user support and troubleshooting for Office365 applications and features
- related to conducting virtual meetings and teleconferences
- Track changes to users and groups
- Management of content uploaded to MS Teams, including data retention policies
- Manage MS Teams settings
- Support, operate, and maintain the Online Services

Who has access to your personal data and to whom is it disclosed?

The personal data is disclosed, under the need to know basis, to the following recipients:

- Display name to any other person within a meeting you may join
- Harrow's IT team to provide the service. Personal data is stored in the EU according to the application configuration implemented. The data is not used for any other purposes nor disclosed to any other recipient.
- Video's of Public democratic meetings are available to stream via Harrow's website or youtube.com after the event.

How do we protect and safeguard your information?

We implement appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. MS Teams has been configured to preserve the confidentiality of the information you exchange by implementing encryption during all communications and in storage, and anonymous access is not authorized. Any information you add to a group in MS Teams, be it via chat, video conference or file sharing, will be available only to the specific users and groups who have delegated access to those files/shared areas.

Who has access to your personal data and to whom it is disclosed?

Harrow IT staff and for your name and email address (if you chose within Microsoft Teams to disclose it) other members of meetings or invites you are party to.

Microsoft data centres are certified in several security standards, most notably ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud.
Microsoft has implemented several safeguards to ensure the availability of the information. As a minimum, data is replicated between two data centres within the same UK region, has redundancy controls and implements backups that are encrypted before being transmitted and stored. Data centres have physical and logical security monitoring measures, such as:

- video surveillance of the perimeter;
- seismic and environmental monitoring at the buildings;
- monitoring of security threats, such as worms, denial of service attacks, unauthorised access, or any type of unlawful activity.

Microsoft has implemented a list of over 700 safeguards in Microsoft's systems, servers, and data centres. This includes safeguards against accidental or unlawful destruction, loss, unauthorised access, use, modification or disclosure. Information is encrypted while at rest and in transit. As mentioned above, Personal data is stored in the UK according to the application configuration implemented by Harrow Council, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

Nevertheless, if access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out.

The following safeguards are implemented:

- In all transfers to third countries, Microsoft uses EU Standard contract clauses for the transfer with its sub processors.
- Microsoft requires sub processors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardise and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft.

How can you obtain access to information concerning you and, if necessary, rectify it? How can you receive your data? How can you request that your personal data be erased, or restriction or object to its processing?

You have the right to access, rectify, erase, and receive your personal data, as well as to restrict and object to the processing of your data, in accordance with Articles 15 to 20 of the General Data Protection Regulations 2016.

If you would like to exercise any of these rights, please send a written request explicitly specifying your query to the Council's Data Protection Officer:

Darren Davies
Data Protection Officer
DPO@harrow.gov.uk

The right of rectification can only apply to inaccurate or incomplete factual data processed within the MS Teams procedure. Your request will be answered free of charge and without undue delay, and in any event within one month of receipt of the request. However, according to Article 12 of the General Data Protection Regulations 2016. That period may be extended by two further months where necessary, considering the complexity and number of the requests. We shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

What is the legal basis for processing your data?

Processing is based on Article 5.1(a) of Regulation (EU) 2018/1725. The personal data is collected and processed in accordance with Harrow Council's Information security policies.

How long do we store your data?

Data will be stored in MS Teams for one year after the exchange activity is completed. Video's published under the transparency act, for example public held meetings saved to YouTube will be available indefinitely or in line with the storage facilities local policies.