1. Introduction

1.1 Background

Monitor has offered Microsoft SharePoint based IT services to Monitor staff over a period of time. Monitor is integrating with 2 other NHS functions: the Trust Development Authority (the TDA) and the patient safety functions of the NHSE (NHSE), to become NHS Improvement (NHSI). Existing IT services within Monitor/TDA/NHSE do not allow for interoperability and/or collaboration between the different NHSI functions.

A trial period using “Kahootz” for collaborative working is being adopted. Kahootz is a cloud based service provided by Inovem Ltd, Data Protection Registration number Z8289153. Kahootz is an entirely new service and therefore a requirement to have in place an Acceptable Use Policy and define the appropriate terms of its use is necessary. The selection of this solution was in line with the overarching Government policy of “Cloud First” and the requirement for services to be provisioned utilising cloud based products. It is also in line with the Government’s procurement policies and expectations under the G-Cloud Framework. It should also be noted that the service has achieved very high international security accreditation and acceptable levels of security certification digitalmarketplace.

1.2 Purpose of this document

This document sets out the requirements and the proposed policy wording for a User Agreement covering all NHSI services.

1.3 Future revisions

It is expected that the requirements described in this document as well as the policy wording will be revisited and revised as appropriate over time.

The policy requirements and wording will also be reviewed in light of any changed or additional policies developed by NHSI or The Department of Health.

2. Policy Requirements

This section sets out the overall requirements to the policy framework including policy scope, objectives and guiding principles.

2.1 Policy scope

The policy framework must apply to all access and use of Kahootz including;

- Email
- Calendar
- Documents & Folders & Databases
- Dashboard
- Blogs
- Community/Forums

The policy framework applies globally at any time whenever a user is logged in.

2.2 Policy objectives

The main objectives of the policy framework are to:

- Ensure that Kahootz is a safe, secure, reliable and efficient system for NHSI staff to perform the business handling material that is not classified, classified as being OFFICIAL or OFFICIAL (COMMERCIAL);
- Ensure that all aspects of NHSI are able to interact and interoperate with other and collaborate together;
- Deter and prevent misuse of NHSI resources (Information, systems and infrastructure);
- Protect users from data loss or unwanted data disclosure and ensure they comply with statutory data protection and handling expectations including the Data Protection Act 1998, the Health and Social Care Act 2012 and the Computer Misuse Act 1990, whilst also meeting the requirement for Kahootz to have an ISO27001 certification and is aligned with emerging NHS Mail standards;
- Clarify and emphasise user responsibilities in the context of the sharing options made available by Kahootz;
- Provide Monitor or the TDA Information Systems Functions with the necessary permissions and user consent to record and maintain administrative user data and to take specified actions on the user's data; and

- Ensure that all users of Kahootz operate within wider legal framework.

2.3 Guiding principles

The policy framework is based on the following guiding principles:

1. **Eligibility and Applying for access** – Anyone applying for access to the service should work for or on behalf of Monitor/TDA/NHSE or must be sponsored by one of these organisations.

2. **The service provided** – Kahootz is fully funded by Monitor and provided to eligible users (as set out in Principle 1). The service does not include support for any Kahootz Web applications, individual hardware, connectivity or third party Apps.

3. **Access devices** – Users may access the service from any compatible device including PCs, laptops, smartphones, tablets or equivalent through apps approved by Monitor/TDA/NHSE IS Function and only in accordance with the User Agreement.

4. **Data ownership** – As per Monitor/TDA registration with the Information Commissioner ICO DP Register and under the Data Protection Act 1998, Monitor and the TDA are the registered Data Controllers for all content on the service and all content is Crown Copyright unless otherwise stated. Users retain responsibility for ensuring that all content they store on the service complies with relevant policies (including those specifically set out in the User Agreement).

5. **Code of conduct** – When using the service and communicating through the service, users shall remember that they act as representatives or partners of NHSI at all times.

6. **Administrative user information** – Users are required to provide permission for Monitor/TDA IS Function to record and store a limited amount of administrative information about the user in order to provide the service.

7. **NHSI access to data** – By using this service Users are providing permission for Monitor/TDA IS Function to conduct automated compliance scans of content created, stored, transmitted or shared on the service and for Monitor/TDA to access any content identified as in possible breach of the law, Monitor, TDA or Department of Health policies. For further information relating to monitoring please refer to Monitors Email, Internet and Telecommunications Policy.

8. **Acceptable use** – The service is provided for the purposes of NHSI activity. Users must comply with the policy clauses in the User Agreement setting out restrictions on the

types of data stored, shared or extracted from the services.

9. **Information security** – In line with a User's terms of employment, Users are required to take all necessary measures to protect all content from loss, theft, corruption or inappropriate dissemination. This includes providing permission for Monitor/TDA IS Function to remotely remove data that is stored on a remote device (such as a smartphone or tablet) that has become lost or stolen.

10. **Service termination** – when a user is no longer eligible for the service or wishes to terminate their use of service, the user account will be suspended and relevant content transferred to a nominated account on the service (nominated by the User in the first instance or by their Line Manager in lieu of this). Emails will be retained for a period of two years and a record of administrative user information will be retained for a maximum period of two years for the purposes of protecting the integrity of the service and security of information.

11. **Inspection and legal hold** – Monitor/TDA may freeze and disclose data held on or related to a user account in the event of a legal investigation.

12. **Enforcement and sanctions** – Where a user is in breach of the policy, we will take appropriate, proportionate action with the ultimate sanction being permanent revocation of the service, reporting the breach to appropriate legal authorities and fully supporting any subsequent investigation or prosecution.

2.4 Policy context

The policy must align with the wider applicable policy context outlined below.

2.4.1 Applicable law

Kahootz is provided by Monitor and is subject to English law.

2.4.2 Related policies

This policy may guide the user to the following legislation, additional policies and third party agreements which they would need to be aware of as a minimum:

- The Data Protection Act 1998;
- The Health and Social Care Act 2012;
- Computer Misuse Act 1990;
- Cloud Technology Solutions (CTS) Privacy Policy;
- Monitor Email, Internet and Telecommunications Policy

2.5 Policy governance

The final policy and future updates to the policy shall be drafted and governed as shown in the table below:

Name	**Role / Title**	**Contribute**	**Review**	**Sign-off**
Pete Sinden	Policy owner / Information Services CIO, Monitor		Yes	Yes
Kirsty Benn-Harris	Information Services Information Governance Manager, Monitor	Yes	Yes	
Hannah Westwood Legal Advice	Senior Legal Advisor, Monitor	Yes	Yes	Yes
Mark Smith	Information Services Head of Operational Systems and IT Support, Monitor		Yes	

Policy issues or questions raised by users shall be dealt with according to the following escalation levels:

Level 1: IG Manager

Level 2: Monitor/TDA IS Function

Level 3: Policy owner

2.6 Monitoring of policy compliance

Responsibility for monitoring compliance with this policy rests with Information Services.

The majority of day-to-day monitoring will be undertaken automatically by Monitor/TDA IS Function. If Monitor/TDA IS Function detects any Incidents or violations of the policy then the Monitor/TDA CIO must be notified within a maximum of 48 hours of the event.

Monitor and the TDA are expected to promote this policy to their staff. Any failure to comply with this policy must be notified to the Monitor/TDA IS function as soon as possible.

3 Policy presentation and acceptance

3.1 Specific Kahootz policies required

Based on the requirements outlined in the previous section this policy is presented as a single User Agreement which includes a section dedicated to Acceptable Use.

The requirement for a broader agreement than just an Acceptable Use policy is the need to obtain explicit user consent for the recording of a small amount of administrative user data and the Monitor/TDA IS Function accessing data, disclosing data to third parties (under exceptional cases such as formal investigation by the authorities) and potentially removing data from external devices.

3.2 Format

The User Agreement is made available to users in a full as well as in summary form.

The full version of the document concisely presents the current obligations of the user completely and unambiguously. The summary version of the document is designed for on-screen reading and highlights key points and the main implications of using the service.

3.3 Implementation

This agreement shall be implemented as follows:

1. The full version of the User Agreement is and will always be available on Kahootz
2. On initial log-in the user is presented with a summary version of the User Agreement and a link to the full User Agreement which the user is required to accept to proceed.
3. On initial set-up of a user account an email with a link to the full version of the User Agreement will be sent to the user (for future reference).
4. Updates to the User Agreement or major changes to the functionality provided is notified to all users on Kahootz

Appendix A

Full wording of the User Agreement

This appendix sets out the wording as presented to the user which they are required to accept in order to access the service. It is based on the requirements and guiding principles described in this document and is included for clarity.

A.1 Definitions

The following definitions shall apply to this User Agreement

Term	Definition
“App”	Shall mean a self-contained program or piece of software designed to fulfil a particular purpose when downloaded by a user to a mobile device or web browser.
“Cloud Technology Solution (CTS) Privacy Policy”	Shall mean: (a) the privacy notice located at Cloud Solutions Privacy Policy
“Device”	Shall mean any form of computing equipment including PCs, laptops, smartphones and tablet computers.
“Acceptable Use Policy”	Shall mean the acceptable use policy for the service located here:
“Privacy Policies”	Shall mean: (a) the privacy notice located at Privacy Policy
Government Security / Protection Classifications	Shall mean the classification structure as set in Monitor Records Classification Procedure until such time as they are updated.
“Information”	Shall mean any content whatever its medium - whether written on paper or stored in any electronic form, hardcopy or otherwise including but not limited to documents, sound, visual or audio-visual recordings.
“Kahootz”	Operates as a multi-tenanted Software-as-a-Supplier within the Public Cloud

“Monitor/TDA IS Function”	Shall mean the Monitor/TDA Information Systems Function
“NHSI”	Shall mean National Health Service Improvement
“Other Sensitive Information”	Shall mean Information other than Personal Confidential Data, Government OFFICIAL (PERSONAL), SECRET information or Government TOP SECRET information that may still result in loss of an advantage or level of security if disclosed to others. This includes Information where loss, misuse, modification, or unauthorized access can adversely affect an individual or a business.
“Personal Confidential Data”	Shall have the meaning as defined in section 6.3 of the Caldicott Information Governance Review (March 2013). This defines Personal Confidential data as personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people. The definition includes ‘sensitive data’ as defined in the Data Protection Act. Refer to HSCIC FAQs for further details.
“Security Measures”	Shall mean the measures put in place to protect Information from unauthorised access. This includes anti-virus software, network firewalls, password protection, screen-locks, encryption and software for enforcing certain Device configuration settings.
“Software Application”	Shall mean a computer programme running on a Device for the purposes of accessing or handling Information. This includes web browsers, email clients and mobile apps.
“The Service”	Shall mean Kahootz cloud computing platform built on **add providing users access to: ● Email; ● Calendar; ● Documents, Folders, Databases; ● Dashboard ● Blog; and ● Community/forums
“Third Party Suppliers”	Shall mean organisations contracted by the Monitor/TDA IS Function from time to time to provide The Service. These organisations are subject to the same terms and conditions as the prime contractor and will operate to the same principles.
“User”	Shall mean the individual person accessing Kahootz

Throughout this User Agreement the terms “include” or “includes” shall be read as “includes but not limited to”.

A.2 About this user agreement

1. This agreement sets out your obligations as a User of The Service. It is designed to protect both you as the User and Monitor/TDA and ensure that The Service is a safe, secure and efficient system to support you in your interaction within NHSI. By accepting this agreement you agree to the obligations described below.

2. Kahootz is provided as a service to you by Monitor.

3. This agreement will be subject to change and you will be asked to review and accept the agreement when it is revised.

4. If you are in breach of this User Agreement or any related policies, Monitor/TDA IS function will take appropriate, proportionate action with the ultimate sanction being suspension of your Kahootz user account and possible reporting of the breach to relevant authorities.

A.3 Scope of The Service

1. This agreement applies to all Users while accessing Kahootz.

2. The Service is available to any member of staff working for or on behalf of or sponsored by Monitor/TDA/NHSE.

3. All Information on The Service is Crown Copyright unless otherwise stated (See Office of Public Sector Information website for information).

A.4 Your obligations and responsibilities

1. You are fully responsible for all the Information you have created, stored, transmitted or shared using The Service and the Monitor/TDA shall not be liable for any such Information.

2. It is your responsibility to familiarise yourself with the terms of this User Agreement as well as any other policies or guidelines that may be applicable to your work or your terms

and conditions of employment.

3. You will remain liable for any additional cost as a result of you purchasing third party applications or services which are not a defined part of The Service.

4. It is your responsibility to ensure that any Information shared with or created by 3rd parties and associated with your Kahootz account complies with this User Agreement. Such 3rd parties may not have seen or have accepted this User Agreement and may choose to share Information further without your consent. Information shared must contain appropriate copyright and confidentiality notices and restrictions. You should make any 3rd parties aware of the consequences of “resharing” data.

5. It is your responsibility to ensure, and provide evidence on request, that all Information you have created, stored, transmitted or shared using The Service complies with relevant policies and legislation. This includes:
    a. this User Agreement;
    b. relevant copyright restrictions;
    c. the Data Protection Act 1998;
    d. the Health and Social Care Act 2012;
    e. the Computer Misuse Act 1990; and
    f. Monitors Email, Internet and Telecommunications Policy.

6. The Service allows you to associate items of personal Information with your user profile which may be seen by other people. This could include your date of birth, education, employment and relationship status. By providing such information you are consenting to it being visible to other users as well as organisations engaged in providing The Service.

7. It is your responsibility to inform Monitor/TDA IS Function if you no longer require The Service.

A.5 Acceptable use

1. **The Service has been recognised as acceptable and secure for the creation, storage and sharing of documents classified as, not marked classified, Government OFFICIAL and OFFICIAL (COMMERCIAL).**
2. **A User may not, under any circumstances, use The Service to create, store, transmit or share any of the following types of information:**
    a. **Personal Confidential Data; and**
    b. **Material classified as Government OFFICIAL (PERSONAL), SECRET or TOP SECRET.** Monitor Records Classification Procedure

3. When accessing The Service from a compatible Device such as a PC, laptop, smartphone, tablet or equivalent you must only do so through Software Applications allowed by Monitor/TDA IS Function.

4. The Service is provided to you solely for the purposes of NHSI-related activity and you may not use The Service for any third-party business purposes.

5. When using and communicating through The Service you act as a representative or partner of the NHSI at all times and this must be reflected in your general conduct.

6. You must not use The Service for any activity which may disrupt, degrade, impair, or violate the integrity or security of The Service or any other third party services. Such activity includes:
    a. attempts to breach Security Measures (including scanning, probing, or other testing or vulnerability assessment activity);
    b. attempts to disrupt services (including generating excessive email traffic or distributing files with malicious content);
    c. intentionally distributing viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
    d. transmission of unsolicited bulk e-mail messages ("Spam");
    e. any activity which may attract excessive use of The Service (including receiving replies from unsolicited e-mails; or attracting excessive traffic to a site hosted by The Service);
    f. any activity that results in the blacklisting or other blockage of NHSI space or email accounts; and
    g. using any part of The Service with forged TCP/IP packet header information.

7. You must not use The Service:
    a. to violate, or encourage the violation of, the legal rights of others;
    b. to engage in, promote or encourage illegal activity;
    c. for any unlawful, invasive, infringing, defamatory or fraudulent purpose; or
    d. to be threatening, abusive or to invade another's privacy including obtaining any improper personal data through our Service, or cause annoyance, inconvenience or needless anxiety or to harass, upset or annoy any other person.

8. You may only send bulk e-mail messages to recipients who have expressly requested receipt of such e-mail messages via a verified opt-in process and you must not continue to send bulk email messages to users who have indicated that they do not wish to

receive them.

9. You may not set-up automatic forwarding of your email to another email account.

10. You are only allowed to retrieve email automatically from email software configured on a device managed and controlled by you or your employer.

A.6 Managing your password

1. You must ensure that the password used to access The Service:
    a. is never disclosed to any other individual or organisation;
    b. is changed immediately after your first log-in or a password reset;
    c. is updated every six months;
    d. is at least 8 characters long and contains a combination of uppercase letters, lowercase letters and non-letter characters; and
    e. does not contain common text strings, dictionary words or personal data such as your username or date of birth;
    f. is unique to your Kahootz account and not identical to any other password used by you to access other computer systems or services.

2. If you know or suspect that any individual or organisation is in possession of your password, you must change it immediately and notify Monitor/TDA IS Function.

3. Where possible, you must disable any automated log-in or local storing (“caching”) of your Kahootz user ID and password. In some circumstances it may be difficult to completely disable this, and you must therefore also ensure that any Device used to log-in to The Service is protected with a Device password.

A.7 Maintaining security of Information

1. In line with accepted good practice, you must take all necessary measures to protect Information from loss, theft, corruption or inappropriate dissemination – regardless of whether Information is stored on The Service or elsewhere.

2. You must ensure that adequate Security Measures are in place on any Device used to access The Service.

3. In case of loss or theft of a Device used to access The Service you must inform Monitor/TDA IS Functions immediately who can assist with deletion of Information from the Device.

4. You should not store, transmit or share Other Sensitive Information (as defined above) unless you have agreed with your relevant manager that it is appropriate to do so and completed a risk assessment.

A.8 Inspection and legal hold

1. Monitor/TDA functions may perform automated compliance scans of Information created, stored, transmitted or shared by you on The Service to identify Information that could be in possible breach of this User Agreement or other applicable policies or laws. Please refer to Monitors Email Internet and Telecommunications Policy for further information.

2. Monitor/TDA functions may freeze, disclose and prevent further access to all Information held on or related to your user account in the event of a legal investigation or an investigation of misconduct.

A.9 End User Consent

1. By accepting this User Agreement you provide permission for:
    a. Monitor and Third Party Suppliers to provide you with The Service as set out in this User Agreement;
    b. Monitor/TDA IS functions to conduct compliance scans and, where necessary, access, monitor, use or disclose Information created, stored, transmitted or shared by you using the service;
    c. Monitor/TDA IS functions to remove Information deemed in breach of this User Agreement or other applicable policies or laws;
    d. Monitor/TDA IS functions to disclose information associated with your account to appropriate authorities;
    e. Monitor/TDA IS functions to store a limited amount of administrative user data about you including your name, organisation, job title, primary contact email and primary contact telephone number.
    f. Monitor/TDA IS functions and Third Party Suppliers to treat your personal data in accordance with UK law, Monitor's agreement with Kahootz, Kahootz Privacy Policies and the Cloud Technology Solutions (CTS) Privacy Policy.

g. Monitor/TDA IS functions and any applicable Third Party Suppliers to disable or suspend your user account if you are deemed to be in breach of this User Agreement;
h. Monitor/TDA IS functions to remotely remove data from a Device used by you to access The Service; and
i. Monitor/TDA IS functions to retain a record of administrative user information for a period of up to two years for the purposes of protecting the integrity of the service and security of information. This is subject to review by The Department of Health.

2. By accepting this User Agreement you agree that Monitor/TDA IS functions may, upon you leaving The Service, transfer ownership of Information associated with your account to another user nominated by you.

A.10 Escalation and Clarification

In the event that you are unclear about your responsibilities and obligations under this User Agreement, you should refer any questions to Monitor's IG Manager or Monitor/TDA IS functions or ultimately the policy owner.

Appendix B

Summary of the User Agreement

This appendix sets out the summary wording which presents the agreement to users in summary form e.g. on first log-in to Kahootz.

Summary

By using this service you agree to comply with the full User Agreement for Kahootz. The full text of the User Agreement is available here (it's the entire doc before this – link to be saved somewhere?)

Key points of the User Agreement include:

- **The Service has been recognised as acceptable and secure for the creation, storage and sharing of documents classified as Government OFFICIAL and OFFICIAL (COMMERCIAL)** Monitor Records Classification Procedure for further details**.**
- It is your responsibility to become familiar with, and make use of, the functionality offered by The Service and to use this in an appropriate fashion. This includes understanding the sharing features available and using these features in a way that is compliant with this User Agreement.
- You may not, under any circumstances, use The Service to create, store, transmit or share any of the following types of information:
    - Personal Confidential Data; and
    - Material classified as Government OFFICIAL (PERSONAL), SECRET or TOP SECRET.
- You may access The Service from a compatible Device such as a PC, laptop, smartphone, tablet or equivalent through Software Applications approved by Monitor or the TDA IS Function.
- The Service is provided to you solely for the purposes of NHSI-related activity and you may not use The Service for any third-party business purposes.
- You retain full responsibility for ensuring that all Information created by you, stored, transmitted or shared by you through The Service complies with all policies set out or incorporated by reference in the User Agreement.

- You are required to take necessary measures to protect all NHSI related content from loss, theft, corruption or inappropriate dissemination – regardless of whether content is stored on The Service or elsewhere.
- By using The Service you grant consent for Monitor or the TDA IS Function and appropriate Third Party suppliers (Kahootz admin) to
    - conduct compliance scans and, where necessary, access Information created, stored, transmitted or shared by you;
    - remove Information deemed in breach of the User Agreement or other applicable policies or laws.
    - store a limited amount of administrative user data about you including your name, organisation, job title, primary contact email and primary contact telephone number.
    - remotely remove NHSI related content (only) from a Device used by you to access The Service when appropriate to do so.
- If you are found to be in breach of the User Agreement, Monitor or the TDA shall take appropriate, proportionate action with the ultimate sanction being permanent revocation of your account, reporting the breach to appropriate legal authorities and fully supporting any subsequent investigation or prosecution.