June 2024

Annual IG Training 2024

Collaboration:

Health Innovation East

Welcome!

Introductions – Your trainers for today:

Tehlana Durity Wingson
Amal Bushara
Avantika Sengupta

What is this training for?

- Make you more confident when handling data
- Examine use cases
- Ask any questions you may have regarding data protection

Why is it important to complete this training?

- Reviewing data protection foundations
- Improving IG practices and processes within HIE

Housekeeping

Things to note before we start…

- **Please mute your microphone**
- **Training will be recorded**
- **Training assessment afterwards**
- **Q&A at the end but feel free to add questions in the chat as we go**
- **All documents that are available can be accessed by this link:** EasternSharepoint/SitePages/InformationGovernance

What is information governance?

Information governance, or '**IG**', is the management of information and data at an organisation.

Who are we?

Information Governance Services (IGS), the DPO and IG helpdesk

eahsn@informationgovernanceservices.com

As DPO and IG helpdesk, we review **policies, incident procedures, DPIAs and general IG queries** and can help with any questions related to data protection and information governance.

What are we going to cover?

Information Governance Training	
Personal Data	Security and Incidents
Risk of Re-identification	Artificial Intelligence
When do we need a DPIA?	Review of New Systems
Contracts	Questions

Personal Data

What is Personal Data?

Personal data means any information relating to an **identified** or **identifiable** person (directly or indirectly).

Personal Data	Pseudonymised Data	Anonymised Data
Name and Surname	Study ID (research project)	Aggregate Data
Birth Date	Month/Year of Birth	Age range
Email Address/IP address	Reference Number	Synthetic Data

Special Category Data

The types of special category data, listed in Article 9(1) UK GDPR, cover personal data that reveals:

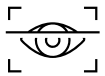

Racial or ethnic origin


Political Opinions


Religious or philosophical beliefs


Trade union membership


Genetic Data


Biometric data to identify a person


Data concerning health


Data concerning a person's sex life or sexual orientation

Where special category data is handled by HIE, it will most likely be health or racial/demographic data.

When can we process Special Category Data?

Under Article 9 of the UK GDPR processing these categories of data is restricted unless one of the below exemptions apply.

- **Explicit consent**
- To carry out the obligations and rights of the controller **for employment, social security, and social protection law**
- Personal data which are **manifestly made public** by the data subject

More likely to apply to HIE as a controller ex. employee relationship

- Necessary for reasons of **substantial public interest**
- **Public health**, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices
- Public interest, scientific or historical **research** purposes
- Preventive or occupational **medicine**, for the assessment of the **working capacity of the employee**, medical **diagnosis**, the provision of **health or social care or treatment** or the **management of health or social care systems and services**

More likely to apply to HIE's partners or in collaborative projects

- To protect the vital interests of the data subject
- Solely relates to the members or former members of a not-for-profit body with a political, philosophical, religious or trade union aim
- For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

Will rarely apply for HIE

Risk of Re-identification

Risk of Re-identification

Even when data is anonymised, if the dataset is large enough or contain significant criteria (age, occupation, residence) it is possible that there will still be a risk of re-identification.

"We use the term 're-identification' to describe the process of turning anonymised data back into personal data through the use of data matching or similar techniques."

- Anonymisation: managing data protection risk code of practice, ICO

When handling data that is de-identified, HIE should exercise caution when using the dataset. In many cases when HIE works with de-identified data, certain measures will be implemented to mitigate the risk.

Example

Is there a risk of re-identification?

An ICS has introduced a new service in their region and has commissioned HIE to conduct a service evaluation.

This project includes HIE receiving anonymised patient level health data from GPs, in addition to patient surveys and interviews.

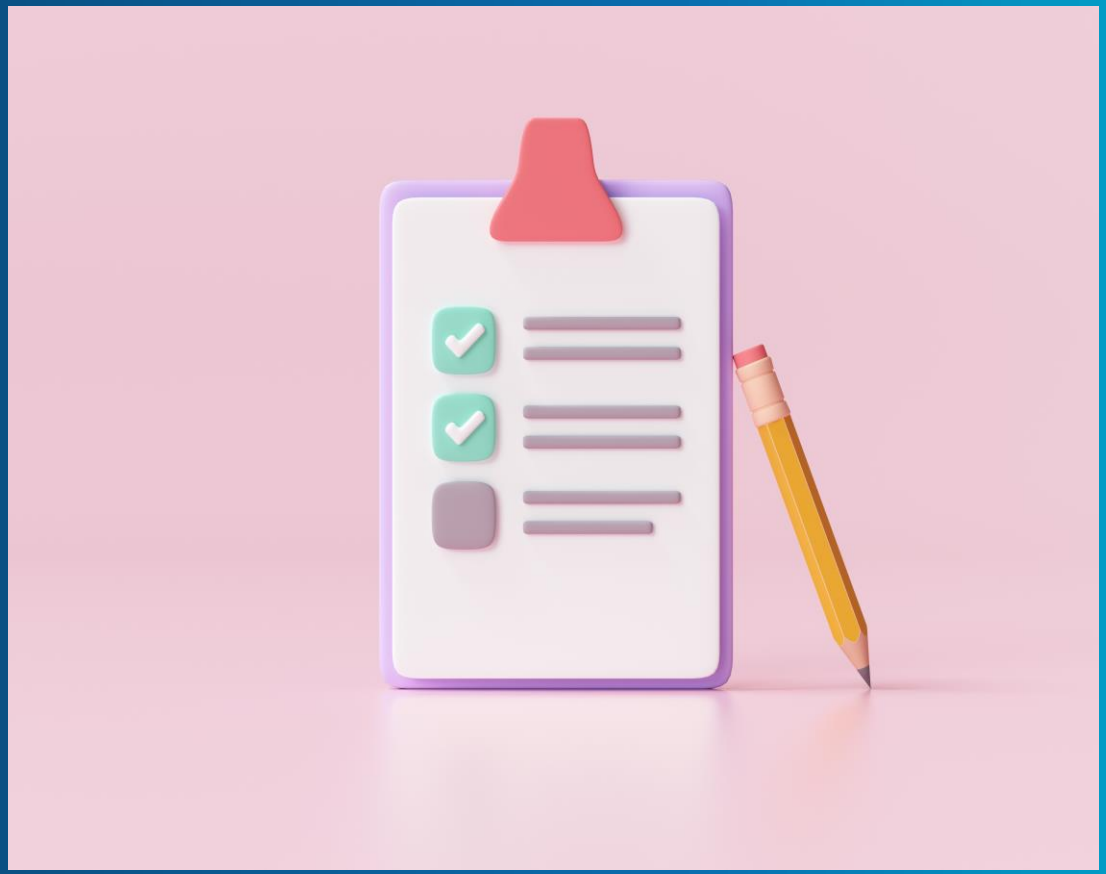
The GP data includes:

- Age;
- Ethnicity;
- Gender;
- Diagnosis;
- Appointments.

Yes!

There will almost always be a risk of re-identification

But there are steps we can take to mitigate this



Risk of Re-identification

There are certain technical and organisational measures that can be implemented to safeguard against re-identification. These include:

- Limiting the use of data, such as deleting small numbers in a dataset
- Contractual clauses to not attempt to link the data, often included in DPA's
- Strict Access Controls
- Participating in IG staff training
- Restrictions on the disclosures of data

When do we need a DPIA

Data Protection Impact Assessment

What is a DPIA?

A DPIA is a comprehensive assessment of a project which processes personal data in order to ascertain the impact of the processing and any associated risks which result from it.

- Demonstrates compliance and accountability *(Art 5(2))* and Privacy by Design *(Art 25) UK GDPR*
- Must be done **before** processing starts
- Is **not** an obstacle to processing, but ensures it is done safely in line with data protection legislation
- Necessary where processing of personal data is likely to be 'high risk'

Find the documents here:

- DPIA Screening Questionnaire: Central Knowledge Bank > Information Governance
- DPIA Template: Central Knowledge Bank > Information Governance

DPIAs and Controllership

One of the key determinants for whether a DPIA is needed is data controllership.

Data Controller	Data Processor
Determines the **why** and **how** of data is used Additional requirements from a data protection perspective ✓ **Responsible for completing a DPIA** ✓ **Responsible for establishing a lawful basis**	Undertakes activities using data **on behalf** of the controller and under their instructions ✓ **Not responsible for undertaking a DPIA** ✓ **Not responsible for establishing a the lawful basis**

Find the documents here:

- FAQs DPIA: Central Knowledge Bank > Information Governance > Data Protection Impact Assessment

Example

Is HIE a data controller?

HIE conducts service evaluations where another organisation **determines** what data will be collected in the process and how the outcome would be used.

For example, evaluating the implementation of the medical device on behalf of a healthcare provider, by conducting patient and staff surveys.

Healthcare Provider

Contracts

Contractual Provisions

Contracts play an important role in keeping HIE compliant with data protection legislation – the organisation's contracts have been drafted with this in mind.

- **Data Processing Agreement (DPA)** - Mandated by legislation in a controller-processor setting;
- **Data Sharing Agreement (DSA)** – Considered best practice in controller-controller setting.

Template contracts **available** if needed along with **guidance documents** on what contract to use.

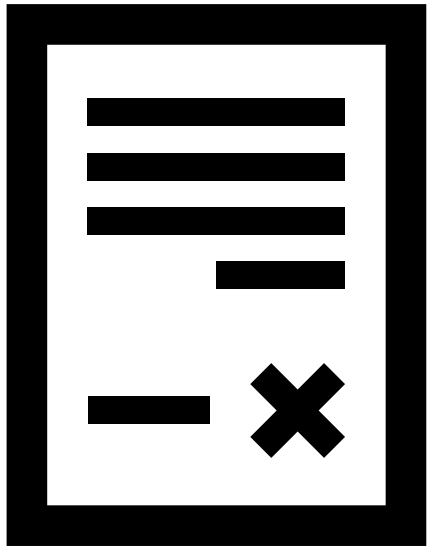
N.B. Before implementing any agreement, whether a DPA or DSA, consider whether there are existing agreements, such as service agreements, with sufficient data protection clauses. In such a case an additional DPA or DSA may not be required.

Contractual Provisions

Other template agreements available for use:

- Memorandum of Understanding;
- Service Agreement;
- Associate Contractor;
- General Terms and Conditions;
- Non-Disclosure Agreement;
- Purchase of Consultancy Services; and
- Sale of Services.

All drafted with **privacy** in mind. 🔒



Security and Incidents

Information security incidents

A security incident is a breach of security leading to the **accidental** or **unlawful**:

- Alteration;
- Unauthorised disclosure;
- Access;
- Loss; or
- Destruction of personal data.

Examples:

- Access by an **unauthorised** third party;
- Sending personal data to the **wrong** individual via email;
- **Unnecessary** or **disproportionate** disclosure of personal data to a colleague;
- Laptop containing personal data being **lost** or **stolen**.

With 72 hours

1. Personal data breach is identified or suspected

2. You fill out section 2 and 3 of the **Incident Report Form** and send to IGS

3. We will fill out remaining sections of the **Incident Report Form** and carry out risk assessment

Your Responsibility

4a. We will advise you on risk mitigation steps (i.e., recalling email incorrectly sent)

4b. We will notify the data protection regulator, and the affected individual where necessary

Appendix A of the Data Breach Standard Operating Procedure 2023

2. About the breach

Please answer these questions as thoroughly as possible:

Question	Response
Please describe what happened Please provide a detailed description of the incident. This overview should provide enough information so that someone who was not aware of the incident can gain a general understanding of what occurred.	
Precisely when did the breach occur? Include the date and time. Depending on the nature of the breach, it may be difficult to pinpoint an exact time and date of occurrence. Such instances should instead be a rough estimate of the date/time.	
Precisely when was the breach discovered? Include the date and time.	
How was the breach discovered? For example, did an incorrect recipient/member of the public make Health Innovation East aware? Did the staff member realise the error that may have been made? How was it brought to your attention?	
Please describe how the incident occurred What was the root cause of the breach? For example, was it due to human error, if so, what was the error? Was it a system malfunction or a failure to comply with existing policies and procedures already in place? Was it a system which was had a design flaw?	
Were there any preventative measures which were in place to prevent an incident of this nature occurring? If so, were they followed? For example, this could be clear policies and procedures, a checklist or potentially a system configuration or some description to help prevent breaches of this nature.	
Was the breach caused by a cyber incident? For example, was the breach caused by unlawful/unauthorised individuals who infiltrated systems including ransomware or a phishing attack?	
What categories of personal data were included in the breach?	

Consider the nature of the personal data that has been impacted and document in this section. Please note that addresses of data subjects are considered to be 'basic personal identifiers' while coordinates are classed as 'location data'. Please give additional details to help us to assess the data in context. For example, health data can range from quite sensitive data to extremely sensitive data. **Please find below examples of categories of personal data:** - Basic personal identifiers, e.g. name, contact details; - Identification data, e.g. usernames, passwords; - Data revealing racial or ethnic origin; - Political opinions; - Religious or philosophical beliefs; - Trade union membership; - Sex life data; - Sex orientation data; - Gender reassignment data; - Health data; - Economic and financial data, e.g. credit card numbers, bank details; - Official documents, e.g. driving licences; - Location data; - Genetic or biometric data; - Criminal convictions, offences; - Other (please give details).	
Number of personal data records concerned? A singular record could be a missing form/list, a notebook or an electronic device. An email on the other hand may have been issued to 20 individuals, this would be therefore classed as 20 records. When assessing the number of data records, consider the nature of the incident and how many records that may be accessible to third parties. In some cases this could be a duplication of the same record (e.g. email).	
How many data subjects could be affected? This relates to data subjects whose personal data has been impacted as a result of the breach, it does not include for example incorrect recipients of another individual's data	
If it was a cyber incident, if the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base	

Phishing

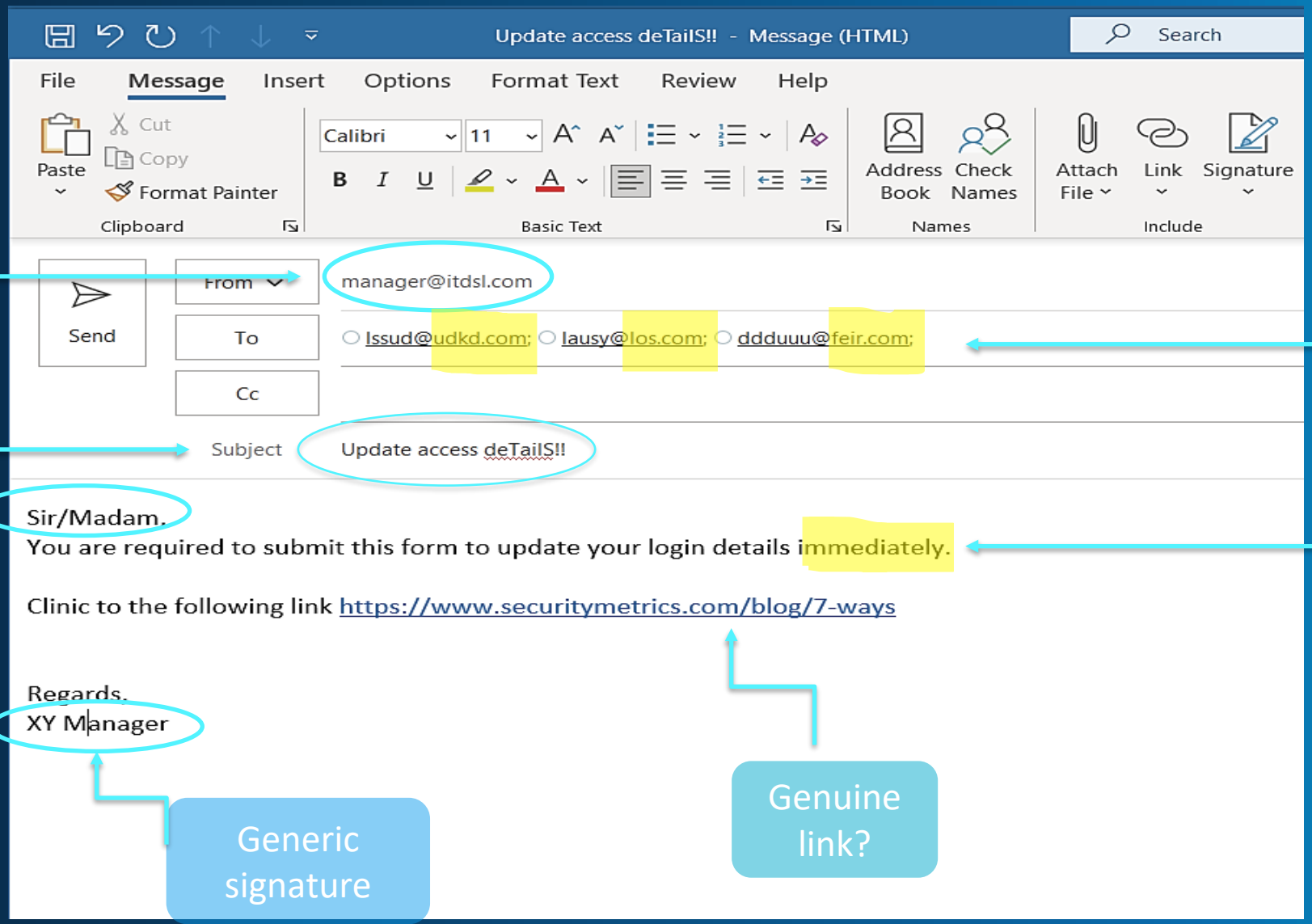
What is it?

Phishing is when attackers attempt to trick users into doing 'the *wrong thing',* such as clicking a bad link that will download malware or direct them to a dodgy website.

Various forms

Can be text messages, social media, or by phone. Most common to happen over email as it can have a huge and wide reach with a relatively low amount of effort for the attacker.

Don’t take the bait



Suspicious sender

Excessive punctuation

Very generic greetings

Inconsistencies amongst domain names

Alarming body

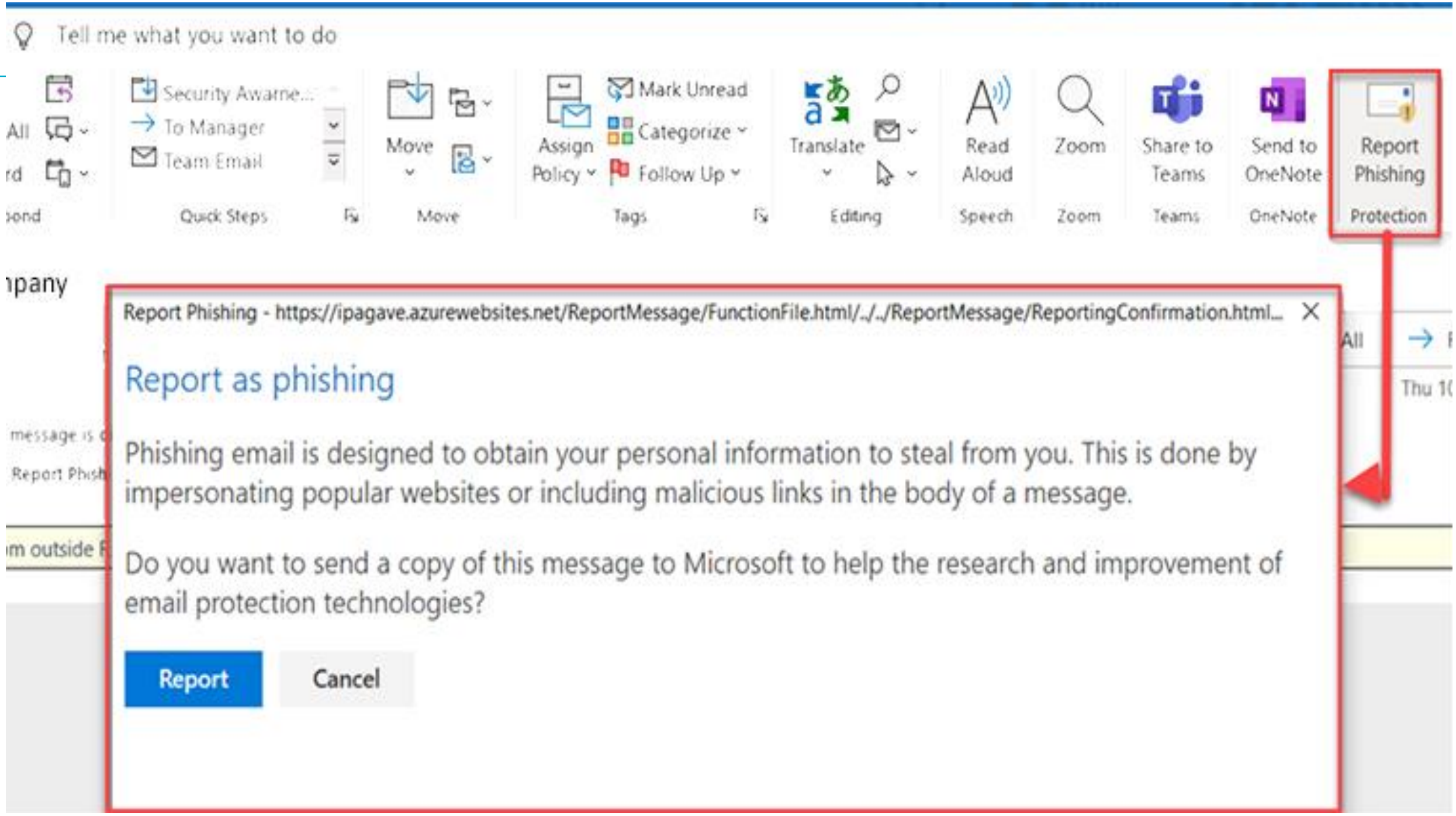
Genuine link?

Generic signature

How to report

If you have received a suspicious looking email, or have reasonable doubts about the legitimacy of the email, follow this process:

- Do **not** open any attachments or click on any links or engage with any response to the sender.
- **Flag** with IT (Data Connectivity) with the subject line "suspicious email" and report using Outlook function.
- IT will then take appropriate action.


Tell me what you want to do
Security Awarne...
To Manager
Team Email
Quick Steps
Move
Move
Mark Unread
Categorize
Assign Policy
Follow Up
Tags
Translate
Editing
Read Aloud
Speech
Zoom
Zoom
Share to Teams
Teams
Send to OneNote
OneNote
Report Phishing
Protection
Report Phishing - https://ipagave.azurewebsites.net/ReportMessage/FunctionFile.html/../../ReportMessage/ReportingConfirmation.html...
Report as phishing
Phishing email is designed to obtain your personal information to steal from you. This is done by impersonating popular websites or including malicious links in the body of a message.
Do you want to send a copy of this message to Microsoft to help the research and improvement of email protection technologies?
Report
Cancel

HIE Policies and their key elements

Data Protection Policy

Key elements:

- Find information on the data protection principles, DPIAs, direct marketing and sharing of personal data

Data Subject Rights Policy

Key elements:

- Guidance on **data subject rights**
- Steps to action valid request
  - Identity verification
  - One month period
  - Log request
  - Check if exemptions apply

Information Technology Policy

Key elements:

- Emails
- Passwords
- BYOD
- Lost/stolen devices

Find the documents here:

- General Documents and IG Policies: Central Knowledge Bank > Information Governance

Artificial Intelligence

Five Principles Governing Use of AI

- Safety, security and robustness;
- Appropriate transparency and explainability;
- Fairness;
- Accountability and governance; and
- Contestability and redress.

General obligations

- Transparency obligation
- Requirement to inform others when:
    - They are subject to a solely automated decision and have a right to object.
    - They are **interacting with a machine.**
    - Their personal data was **used to train and test** an AI system.

General obligations (continued)

- Obligation to ensure that the AI systems have been reviewed to address **human rights-related concerns**.
- Use professional skepticism and be cautious of accuracy.
- Undertake training if provided by the supplier.

Permitted Use

There are specific rules regarding using personal data within an AI system.

Some AI systems are likely to be a threat to individuals' fundamental rights and should be **forbidden**, these include:

- Cognitive behavioural manipulation of people of vulnerable groups such as children;
- Social scoring classifying individuals based on their behaviours, status, or other personal characteristics;
- Real-time biometric identification, such as facial recognition and categorization of people.

Staff are prohibited from using systems to process personal data without the review of the DPO.

Permitted Use

There are specific rules regarding using corporate data within an AI system.

- Staff should confirm whether the AI system includes any third-party **add-ons.**
- Staff should **minimise and limit** the input of **confidential or sensitive information** related to HIE as an organisation, or any of its employees or clients, into the AI application.
- Staff should protect confidentiality of data related to HIE by using labels that prevent copying specific information or through manually **removing references or specific data** related to HIE within the dataset.

Permitted Use

Health Innovation East

Artificial Intelligence Policy

Document Owner	Data Protection Officer, Health Innovation East
Author/s	Information Governance Services Ltd
Version	3.0 Draft
Issue Date	June 2024
Date of Next Review	June 2025
Approved by	BOD

Table of contents:

New AI System Approval Form

GENERAL INFORMATION	
Name and purpose of the product	
Data that will be used in the system	☐ non corporate and non personal data ☐ sensitive corporate/commercial data ☐ personal data
Number of accounts/licenses defined	☐
Review of costs	☐
Use case identified and scope validated	☐
Link to the website and T&Cs of the supplier	
Has the AI supplier been subject to any litigation, regulatory action, or disputes regarding their product?	
Warrantees regarding performance and security	
Measures to protect the confidentiality of the information outlined above	
IT SECURITY RECOMMENDATION	
☐ recommended ☐ not recommended	*[Comment]*
DATA PROTECTION RECOMMENDATION	
Screening questionnaire	☐
DPIA (where applicable)	☐
☐ recommended ☐ not recommended	*[Comment]*
CORPORATE/SMT SIGN OFF	
☐ approved ☐ not approved	

Example of solutions evaluated – DSE Workstation solutions

	Red Flags	Green Flags
Vitrue Health		• AI technology measures teams' posture and ergonomics automatically in 5 seconds.
WorkHappy		

Example of solutions evaluated – DSE Workstation solutions

	Red Flags	Green Flags
Vitrue Health	• Lack of information regarding the AI algorithm. • Inconsistent information about the storage of customer data. • No guarantees regarding the result of the AI algorithm calculation. • GDPR logo is not an official GDPR certification.	• AI technology measures teams' posture and ergonomics automatically in 5 seconds.
WorkHappy		

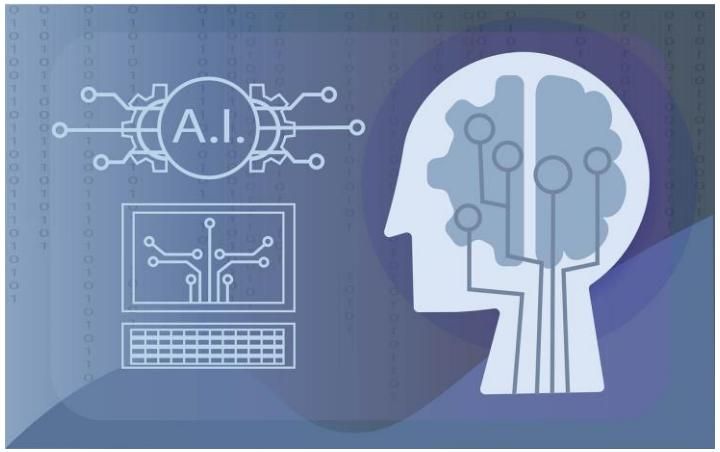
Example of solutions evaluated – DSE Workstation solutions

	Red Flags	Green Flags
Vitrue Health	• Lack of information regarding the AI algorithm. • Inconsistent information about the storage of customer data. • No guarantees regarding the result of the AI algorithm calculation. • GDPR logo is not an official GDPR certification.	• AI technology measures teams' posture and ergonomics automatically in 5 seconds.
WorkHappy		• Detailed information is provided regarding how data is stored, access control, security measures. • Assessment undertaken by professionals who are qualified assessors.

Example of solutions evaluated – DSE Workstation solutions

	Red Flags	Green Flags
Vitrue Health	• Lack of information regarding the AI algorithm. • Inconsistent information about the storage of customer data. • No guarantees regarding the result of the AI algorithm calculation. • GDPR logo is not an official GDPR certification.	• AI technology measures teams' posture and ergonomics automatically in 5 seconds.
WorkHappy	• Difficulty accessing the Privacy Notice due to technical issue.	• Detailed information is provided regarding how data is stored, access control, security measures. • Assessment undertaken by professionals who are qualified assessors.

Generative AI



The use of generative AI should only be allowed where:

- ✓ No personal data has been used to generate content;
- ✓ No copyrighted data, or data subject to any other intellectual property restrictions, has been used to generate content;
- ✓ The fact that the content has been generated by AI is clearly disclosed, whether the generated content is text, visual, audio or video;
- ✓ The sources used to generate are identifiable and documented.

Third-party service providers

It is possible to engage other organisations to process personal data on behalf of HIE. But there are a few conditions that need to be met:

1. The organisation must provide HIE with **sufficient guarantees** that they implement appropriate technical and organisational measures so that the processing will meet the requirements of the UK GDPR.

2. It must be clear which of the parties is **expected** to provide the **training data** for the AI model; and how the intellectual property rights are **assigned**.

Review of New Systems

When do solutions need to be reviewed?

Examples of **low-risk** activities/where HIE is the **processor**:

- Inviting people to participate in an event.
- Conducting surveys, gathering feedback.
- Organising/inviting NHS staff or patients to participate in interviews, workshops or focus groups.
- Conducting service evaluations where another organisation determines what data will be collected in the process and how the outcome will be used.
- Facilitating relationships with suppliers and stakeholders, and day-to-day business operations.
- Managing HR-related necessary activities.

When do solutions need to be reviewed?

Examples of **high-risk** activities/where HIE is the **controller**:

- Designing, collaborating, carrying out evaluations for purposes identified by HIE.
- Implementing new software that involves new forms of data collection and use or which involves sensitive personal data.
- Combining personal data obtained from publicly accessible sources to create a detailed picture of an individual.
- Invisible tracking of individuals via social media plug-ins without adequate consent.
- Employee monitoring.
- Making decisions regarding whether a patient is eligible for individual funding request without any human involvement.

Questions?

Thank you!

For any questions could not be covered today,
please contact us at:

eahsn@informationgovernanceservices.com