**General Data Protection Regulations (GDPR)**

**Staff handout**

**What is the GDPR and what does it mean for/to you?**

The GDPR is a set of guidelines for the collection and processing of personal information of individuals within the EU; it will come into effect in the UK from 25 May 2018, taking the place of the Data Protection Act (DPA), and will not be affected by the UK’s decision to leave the EU.

The aims of the GDPR are to:

* Update the data protection law to take into account new technologies
* To strengthen the data protection laws
* To ensure effective protection of personal data
* To increase penalties for non-compliance
* To embed the concept of privacy by design *(considering data protection right at the start – new technologies for example)*
* Introduce the concept of *‘respect for the essence of the right to data protection’*

The GDPR applies to the following:

* **Data subject** – an individual who is the subject of personal data *(child or adult – everyone involved in this school and our Trust – children, staff, parents/carers, governors).*
* **Data controller** – an organisation or body that is responsible for complying with the Data Protection Law. Determines the purpose and mean of holding and processing the personal data - *(the School and the Trust)*
* **Data processor** – any person who processes data on behalf of the data controller *(for staff data – your Headteacher, Office Manager, Admin and Trust. For children – all of you!)*

**Personal data**

Personal data has a more detailed definition not just name, address, DOB, National Insurance Number etc but also information such as online identifiers (e.g. IP addresses) will now be classed as personal data. The regulations apply to both automated personal data and manual filing systems where personal data can be accessed. To process data we need to ensure that all the following principles have been considered:

**Data Protection Principles (Article 5, EU GDPR) – ‘personal data’ shall be (see Hoop 1 below):**

1. Fair, lawful and transparent
2. Held for specific, explicit, legitimate purposes
3. Minimised - adequate, relevant, necessary
4. Accurate, where necessary up-to-date
5. Retained – storage limitation
6. Secure – integrity and confidentiality

**‘Special Data’** – information that relates to a particular characteristic of a living individual *(e.g. racial or ethnic origin, medical, criminal, sexual, TU membership, religious beliefs, political opinions etc)*

**Lawfulness of Processing (Article 6, EU GDPR) – Hoop 2 (see below) what is our reason for processing? We need one of the following:**

1. Consent – the individual has given consent *(you should all have received a letter)*
2. Performance of a contract *(employment contract for example)*
3. Legal obligation – DBS *(safeguarding/safer recruitment for example)*
4. Vital Interests - life or death *(emergencies)*
5. Public interest/exercise of authority *(Police, Immigration)*
6. Legitimate interest (not for local authorities and schools)

**Purpose of Processing (Article 9, EU GDPR) – ‘special data’ Hoop 3 (see below)**

1. Consent
2. Employment/social security/social protection obligations
3. Vital interests *(life or death)*
4. Non-profit bodies
5. Processing made public by data subject
6. Legal claims
7. Substantial public interest
8. Health, social care, medicine
9. Public interest for public health *(disease)*
10. Archiving, statistics, historical research

**Consent**

You have to give us your consent and this **must** be: freely given, specific, informed and an unambiguous indication of your wishes. Consent **cannot** be obtained from the following: silence, pre-ticked boxes or inactivity.

We have to ensure that we have provided simple and accessible ways for individuals to withdraw their consent.

Special personal data will only be processed fairly and lawfully as required by the first data protection principle if at least one of a number of ***additional*** conditions is satisfied (Article 9).

**Exemptions**

Personal data can be exempted from the duty to process information fairly and lawfully to the extent necessary for making a disclosure: crime prevention; immigration; legal proceedings/court.

**Your Rights**

The GDPR has created new rights for individuals, whilst strengthening some that existed under the DPA; these rights are:

**1. The right to be informed** – this includes our obligation to provide fair processing information, usually in the form of a privacy notice *(your letter)*.

**2. The right of access** – where an individual has requested access to their personal data, we must provide a copy of this free of charge. However, if the request is manifestly unfounded or excessive, we can charge a fee. Under the GDPR, information must be provided within one month of the request. If we refuse your request, we must tell you why and inform you of your right to complain to the Information Commissioner’s Office (ICO).

**3. The right to rectification** – you are entitled to request your personal data to be rectified if it is inaccurate or incomplete. Again, requests must be responded to within one month from the date the request was received, or extended to two months if the request is complex.

**4. The right to erasure** – this enables you to request the removal of personal data where it is no longer required for the process it was originally obtained for. Requests can be refused for reasons such as compliance with a legal obligation or to exercise the right of freedom of expression and information.

**5. The right to restrict processing** – you have the right to ‘block’ or suppress the processing of personal data. In an instance where processing is restricted, we may store the personal data; however, we may not process it any further.

Circumstances that will require the restriction of processing personal data include:

* When an individual has challenged the accuracy of the personal data – processing should be restricted until accuracy is verified.
* When an individual has objected to processing that had been necessary for the purpose of legitimate interests, you may consider whether your organisation’s legitimate grounds override this.
* If the processing is unlawful and the individual has requested restriction instead of erasure.
* If your organisation no longer requires the data, but the data is needed by the individual to defend or carry out a legal claim.

Individuals must be informed when we lift a restriction on processing.

**6. The right to data portability** – this allows you to obtain and reuse your personal data for your own purposes; you are able to move, copy or transfer personal data easily, in a safe and secure way.

**7. The right to object** – you may object to processing based on legitimate interests. We must stop the processing unless we have legitimate grounds that would override the interests, rights and freedoms of you, or if the processing is for the exercise or defence of a legal claim.

You may also object to having your data processed for direct marketing purposes. In both instances mentioned here, we must inform you of your rights in your privacy notice, and at the first point of contact.

**8. Rights to automated decision-making and profiling** – the GDPR ensures that individuals’ data is protected against the risk that a potentially damaging decision is made without human intervention. Rights to automated decision-making and profiling will not be used in school settings.

**Processing Children’s Data**

The GDPR has introduced new provisions that are intended to enhance the protection of children’s personal data. Where services are offered directly to a child, privacy notices must be written in a clear, age-appropriate way *(all parents/carers have received a letter – similar to yours)*.

The GDPR states that a pupil under the age of 16 cannot give consent for themselves – consent must be obtained from a person holding ‘parental responsibility’ *(identity may be checked)*.

Consent from a parent or guardian is not required where the processing is related to preventative or counselling services that are offered directly to a child.

**Accountability and Governance**

Under the GDPR, we (meaning Schools and the Trust) are expected to put comprehensive, but proportionate, governance measures in place that minimise the risk of data breaches. We can demonstrate our compliance with the new accountability principle in the following ways:

* Implementing internal data protection policies: acceptable use agreements, emails, remove access/mobile computing, records and retention, staff training etc.
* Maintaining relevant documentation and processing activities.
* Appointing a DPO – Jill Wilkinson.
* Implementing measures that meet the principles of data protection by default, including data minimisation and transparency.
* Using data protection impact assessments (DPIAs) where appropriate *(new technologies).*

We have more than 250 employees, so we must maintain additional internal records of our processing activities *(we have an Information Register – outlining all the personal data – the who, what, where, how long, etc)*.

**Data Breaches (or Incidents)**

We are required to report any data incidents or breaches that are likely to result in a risk to the rights and freedoms of individuals to the relevant supervisory authority and, if necessary, the individuals affected. An investigation will then take place. If it is deemed a ‘breach’, we have to inform the ICO within 72 hours.

Failure to report a breach in this time will result in a significant fine of up to **€20 million, or 4 percent of the organisations’ global turnover.**

**Consequences:** physical harm, distress, embarrassment, financial loss, identify fraud, reputation.

**Examples of a breach:**

* Website security – personal data accessible;
* Unprotected emails – personal data accessible;
* Lost or stolen USB, iPads, phones, any portable device that may have personal or special data on – photos, progress data.
* A child’s information being sent to the wrong address – annual reports.
* Hacking through weak security/passwords – personal data accessible.

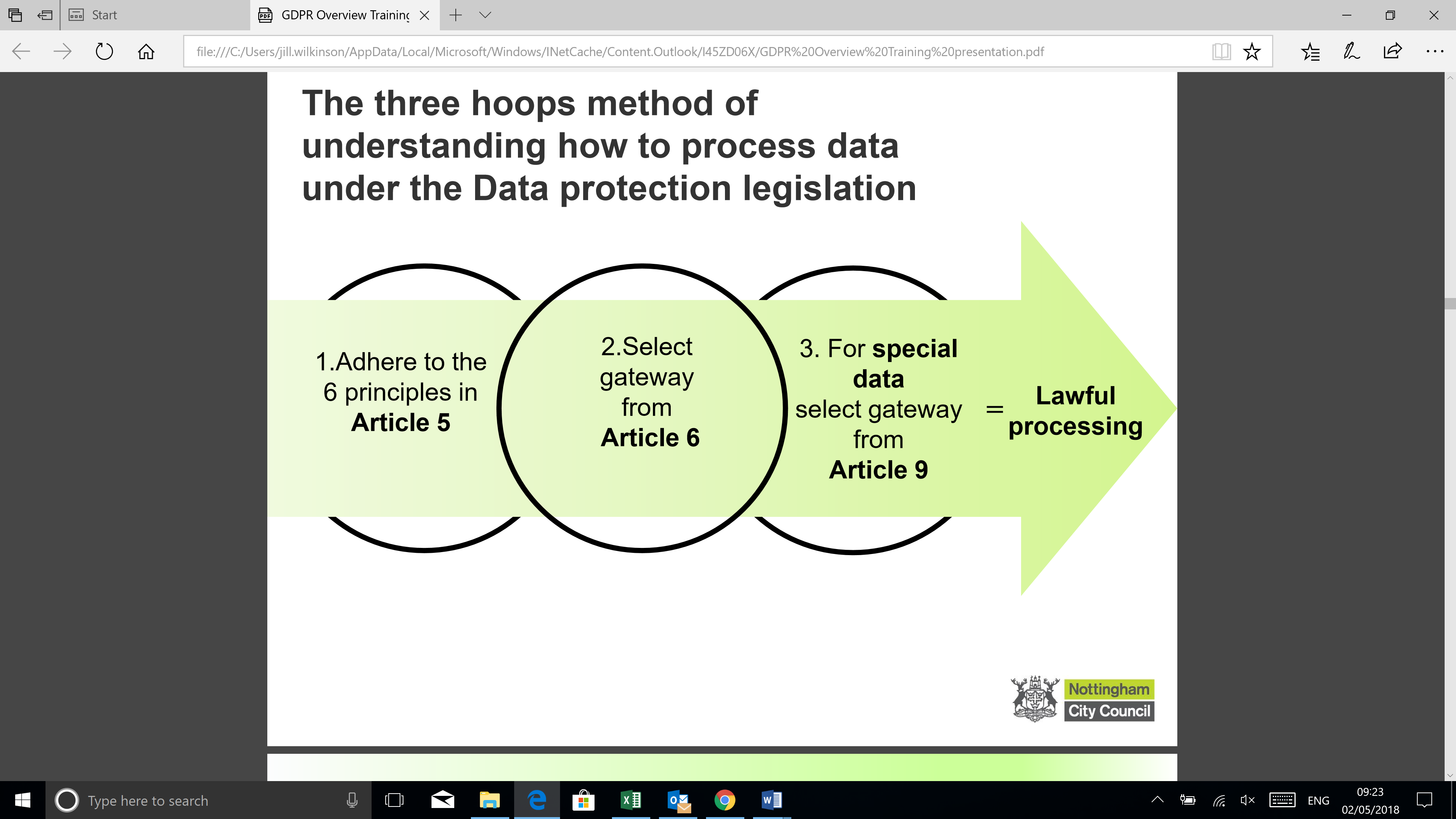
*“A teacher has used an unencrypted memory stick to export some school reports so she can work on them at home on her home computer. The reports include behaviour information which affect children’s progress. A virus in the computer auto uploads the report onto the web and is now visible to all”.*

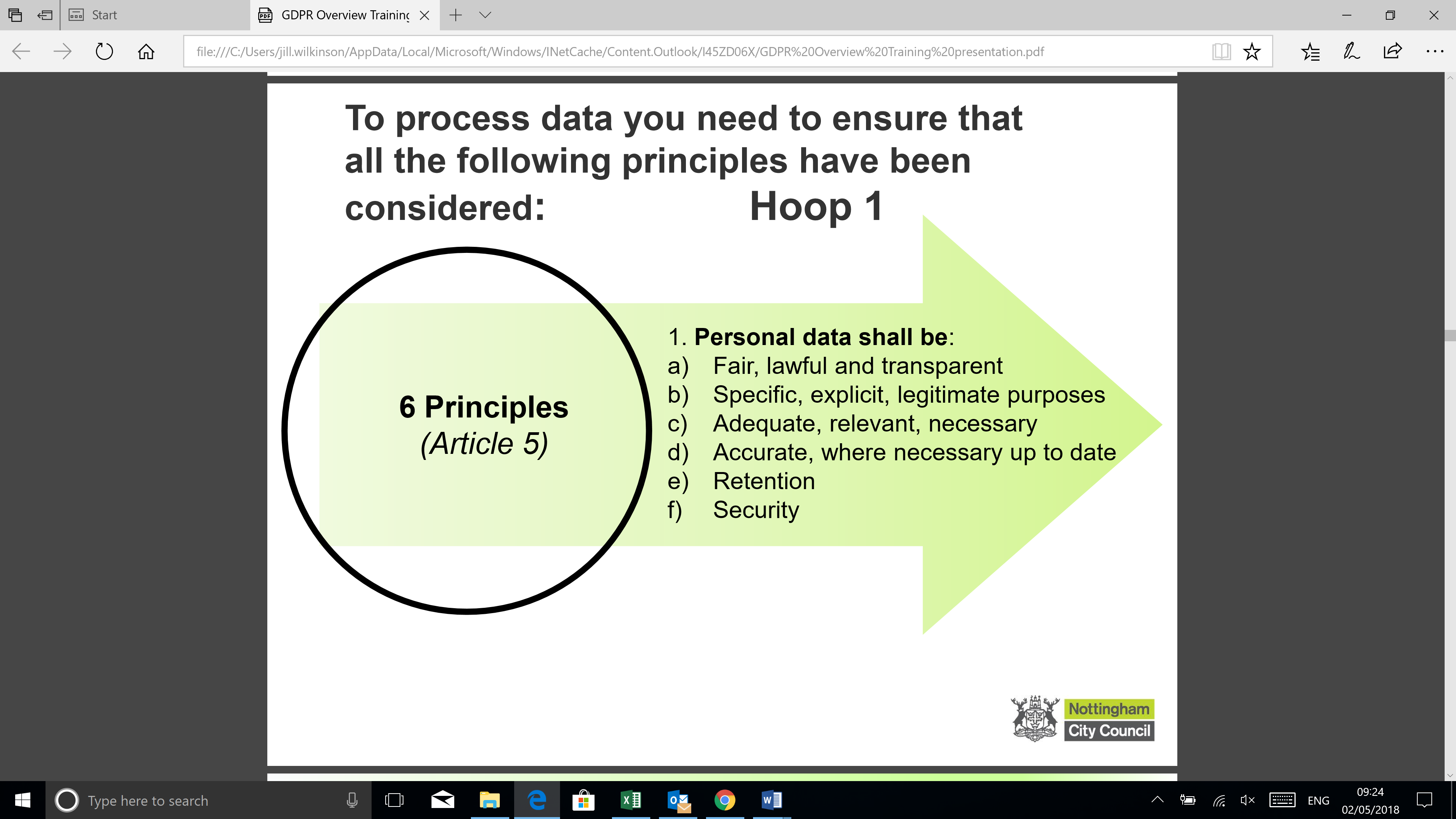
This would be classed as a breach that we would need to report to the ICO. It may result in disciplinary action being taken. The Trust would receive a visit from the ICO to check our procedures and the ICO could issue a fine.

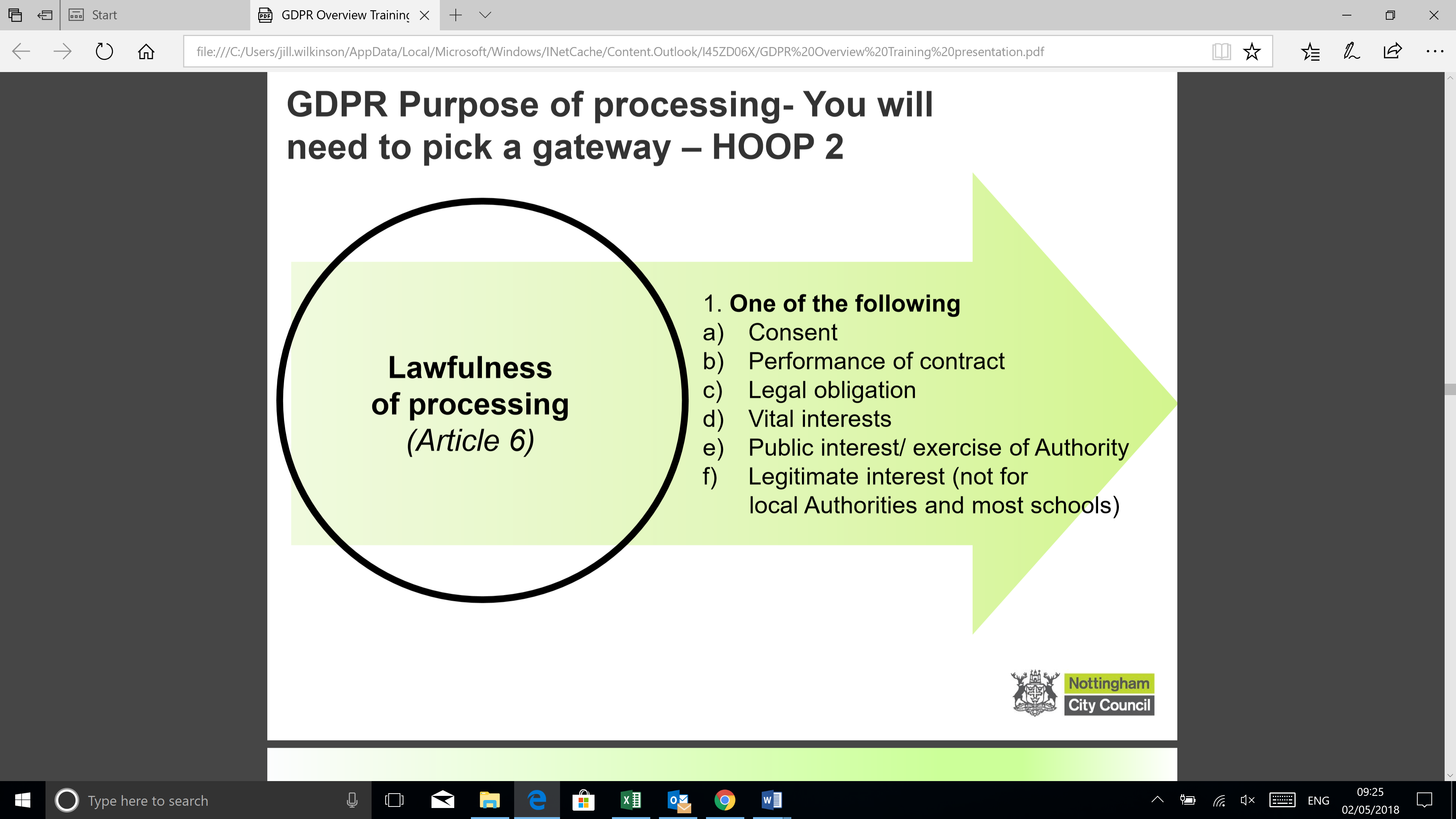
**What can you do? Don’t panic just be sensible**

**Think before you share any personal or special category data with anyone. Do I need to share this – do they really need it – legal or business need? What purpose is it for? Who am I sharing it with? Do we have consent? CHECK IF YOU ARE NOT SURE**

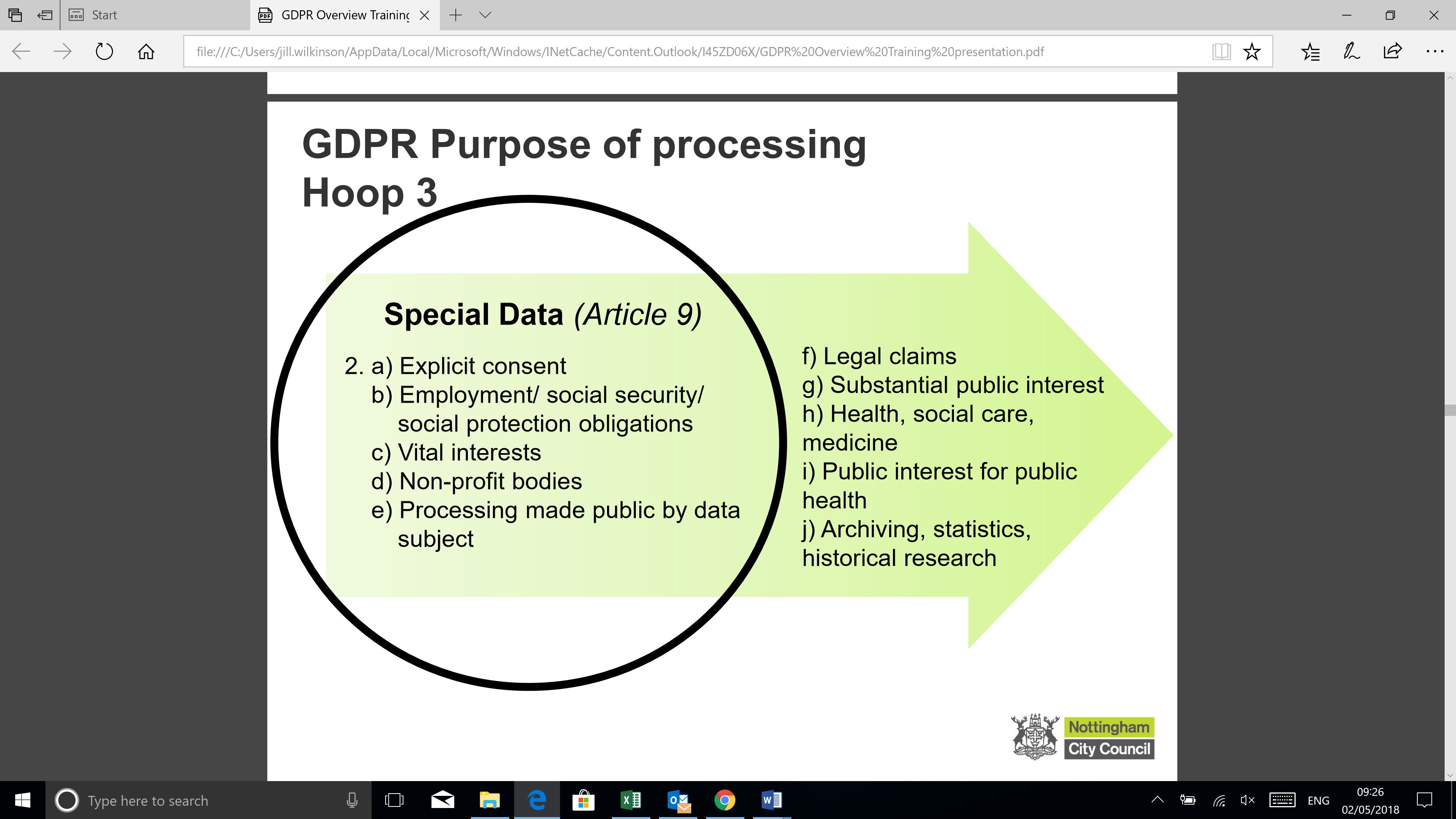
The 3 hoops method of understanding how to process data under the data protection legislation – your Data Processor will help guide you through these hoops or be able to advise if personal or special data can be used.







For example, going on a school trip and the centre asks for medical information of the pupils – they would need this in order to fulfil their contract so yes this can be shared under b, and consent is also likely to have been obtained so a.



So you may have really old photos of children on your school wall on display or really old visitor books with names and photos etc, these may be retained under j. archiving and historical purposes.

**Practical steps you can take to safeguard personal and special category data:**

1. Check you have consent to process this data – your Data Processor will advise you on this. Consent will definitely be needed for photos, videos, marketing, trips, fundraising for both children and staff. The consent should be separated into specific use i.e. for newsletters, for website, for school plays, school trips and for marketing purposes. If you are unsure, use the hoops to help you and definitely seek advice.
2. Encrypt emails where possible. If your school uses Schools IT this is possible now. If your school uses AIT this is coming soon. If you school uses another IT provider you will need to ask them.
3. Check that the ‘auto’ function when you type in your email address uses the correct email – many emails have been sent to wrong addresses because of auto function – turn this off if you can or speak to your IT provider to do this for you.
4. Ensure documents are password protected and ‘lock’ the document. If you are sending via email – in school, school-to-school, school-trust encrypt as well – three layers of security. Locking the document shows you have taken measures from it being edited/altered. If you do not know how to do this, ask your Office team who should know.
5. Annual reports – use a watermark to show that it is a ‘parent copy’ of the report. Letters to NHS, Housing, Benefits – again use a watermark to show who the document is meant for. Again, ‘lock’ the document so that it cant be edited or altered.
6. Change your password regularly. Do NOT share your passwords or use duplicate passwords.
7. Lock your screen or close your computer when away from your desk. Take care when travelling and working on trains as to who may have access to your screen if you are working on personal or special category data.
8. Make sure any sensitive files are locked away in a cupboard.
9. Only use school-issued USBs/external hard drives for school work. These should either be encrypted or have a PIN.
10. Wherever possible, do not leave your devices or files in your car in sight. If you have no alternative, put them in your boot and be aware who might be watching.
11. School Trips – use lockable bags to hold sensitive data. Only use school-issued devices when on school trips for taking photos etc.
12. CHECK AGAIN.

**What to do in the event of an incident or breach?**

1. Notify your Headteacher (Data Controller) or Data Processor (Office Manager) or Data Protection Officer (Jill Wilkinson) as soon as possible. Remember if it’s a breach we have to report it within 72 hours at the point at which we know it’s a breach. An investigation will then follow.
2. If it’s a high risk breach – we must notify the person whose data has been affected immediately.
3. Identify any steps that can be taken to minimise the damage – can it be retrieved, removed etc.
4. Determine exactly what information and to whom it has be released.
5. Identify who may be affected.
6. The DPO or Headteacher may need to notify the ICO within 72 hours it is a personal data breach.

**Mistakes happen and we are here to help.**

**The Trust’s Data Protection Team**

**Data Protection Officer – Jill Wilkinson** The DPO is not required to have any specific qualifications but should have professional experience and knowledge of data protection law.

**Data Controllers – all Headteachers**

**Data Processors – Office/Business Managers**