**COLLABORATIVE RISK**

1. An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet. Many businesses and educational facilities require that employees or students sign an acceptable use policy before being granted a network ID **EXAMPLE** : Use e-mail, social networking sites or tools, or messaging services in violation of laws or regulations or to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or User ID
2. A copyright is a type of intellectual property that gives its owner the exclusive right to copy and distribute a creative work, usually for a limited time. The creative work may be in a literary, artistic, educational, or musical form
3. Software intellectual property, also known as software IP, is a computer code or program that is protected by law against copying, theft, or other use that is not permitted by the owner.
4. The term “public domain” refers to creative materials that are not protected by intellectual property laws such as copyright, trademark, or patent laws. The public owns these works, not an individual author or artist. Anyone can use a public domain work without obtaining permission, but no one can ever own it.
5. Fair use is a legal doctrine that says you can reuse copyright-protected material under certain circumstances without getting the copyright owner's permission.  any copying of copyrighted material done for a limited and “transformative” purpose, such as to comment upon, criticize, or parody a copyrighted work. Such uses can be done without permission from the copyright owner. the fair use of a copyrighted work, including such use by reproduction in copies … for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship or research, is not an infringement of copyright
6. GDPR : The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area

**What are the 7 principles of GDPR?**

**The UK GDPR sets out seven key principles:**

* Lawfulness, fairness and transparency.
* Purpose limitation.
* Data minimisation.
* Accuracy.
* Storage limitation.
* Integrity and confidentiality (security)
* Accountability.

**EXPLAINATION**

(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

(g) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)

**FAILURE TO COMPLY /IMPLICATIONS**

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.