Adopted by Board On 26/6/2018
Reviewed On 4/12/19

# Oasis Church Chelmsford - Information Risk Policy

**Leadership and Governance**

We, the Trustees of Oasis Church Chelmsford are Data Controller of all personal data we process. We use 'consent' as our lawful basis for processing personal information. We have considered our appetite relating to information risks and have agreed it is low. All decisions on how to manage information risks within Oasis Church Chelmsford are derived from our wish to maintain a maximum low level of risk.

We have allocated specific roles with information governance responsibilities across Oasis Church Chelmsford including Senior Information Risk Owner. These roles provide a clear structure for the strategic governance and operational management of information risks within Oasis Church Chelmsford.

The Trustee Board oversee the effectiveness of the information risk policy and are responsible for ensuring improvements are made where necessary.

Each year, we describe our approach to managing information risks within Oasis Church Chelmsford in our annual report.

**Information risk management**

The Senior Information Risk Officer (SIRO) of Oasis Church Chelmsford is responsible for ensuring the information risk policy is implemented. The SIRO is also responsible for ensuring that all significant information risks are considered, managed and documented. The SIRO will gather together an appropriate team of individuals to perform these tasks and will refer more important and/or more complex decisions to the Trustee Board as appropriate.

SIRO approval is required before proceeding with any activity likely to generate a significant information risk to Oasis Church Chelmsford. The decision whether to accept, avoid, transfer or mitigate against the likelihood or impact of an information risk will be based upon the information provided in a Data privacy impact assessment, together with consideration of Oasis Church Chelmsford's defined risk appetite.

All information risk decisions, actions, progress and risk assessments will be recorded for reference, education and compliance purposes.

**Data handling – through life Information Governance measures**

i) Access control

We employ the 'need to know' principle of minimised access to confidential data, set out in the Cabinet Office's 'Minimum Data Handling Measures' when providing access to confidential data. This ensures that all staff and volunteers only ever have access to the minimum amount of confidential data required to perform their valid business role and for which appropriate consent or other lawful basis exists.

We implement the 'need to know' access principle through the establishment of effective ICT user account management processes; by limiting the number and use of privileged accounts and by monitoring the use of ICT systems and limiting access to other physical areas which house

confidential data.

ii) Data classification

We ensure that all staff and volunteers can easily identify confidential data by clearly labelling the document in the header or document watermark as 'CONFIDENTIAL' .

iii) Data in transit: email, fax, post

We ensure via initial and refresher training that all staff and volunteers understand that Oasis Church Chelmsford is legally responsible for the security of data sent whilst in transit, including but not limited to data sent via email, webchat, fax, video, mobile applications and post. We ensure that any email containing confidential information is adequately secured.

iv) Retention, deletion and secure disposal

We ensure that all copies of confidential data are securely erased or destroyed at the end of their 'life'

v) Removable media

We mitigate against the high risks of potential data loss associated with the use of removable media (laptops, USB sticks, DVDs, CDs etc.) by avoiding the use of removable media wherever possible and, where its use cannot be avoided, by ensuring that media is adequately encrypted with a secure password.

vi) Personal data in the cloud or externally hosted
Oasis Church Chelmsford does store personal data in the cloud or externally. Where personal data is stored or processed externally a data privacy impact assessment is undertaken and the ICO Cloud Computing guidance is followed.

vii) ICT

We ensure that Oasis Church Chelmsford implements any necessary IT Security as set out in National Cyber Security Centres 10 steps to Cyber security.

viii) Physical security

We protect the physical locations where confidential data is held using a number of layers of security. We ensure that each staff member or volunteer receives initial and refresher training to confirm they understand the importance of their role in maintaining the 'layers' of physical security that they have control over – as no single person controls all elements, teamwork is essential.

ix) Location of personal information
Oasis Church Chelmsford identifies where all personal data is processed and stored and aims to keep this within the UK or within Europe. Data processed outside Europe, for example by a US based cloud services provider, must make reference to how security requirements for this type of transfer are met in a written contract or data processor agreement.

We ensure that confidential data assets are managed properly by documenting our information assets in an information asset register. We ensure that the data flows of information for that asset are known and

documented ensuring data privacy impact assessments are carried out in high risk areas.

Each asset has an Information Asset Owner designated who has responsibility for the security and business use of the asset.

We employ joining and leaving checklists to ensure that confidential data assets are returned and access to any information is removed when someone leaves Oasis Church Chelmsford.

We ensure all staff, volunteers and contractors successfully complete appropriate data protection training and are made aware of the importance Oasis Church Chelmsford places upon looking after the confidential data entrusted to it.

This training is carried out prior to being given access to confidential information and this is refreshed annually. Roles with additional responsibilities, such as Information Asset Owners, are additionally required to successfully complete advanced training. Successful completion of training is documented and monitored by the Office Administrator. Failure to comply is escalated to the SIRO, and if necessary the Trustee Board, until resolved.

We ensure our staff and volunteer policies are kept up to date to help implement Oasis Church Chelmsford effective management of information risks. Our acceptable use policies require all staff to keep confidential data safe.

All staff and volunteers received training so they know that data security breaches caused by their actions may result in disciplinary or equivalent volunteer proceedings which in some cases may be considered gross misconduct, and that some instances may be criminal offences under Section 55 of the Data Protection Act 1998 or legislation equivalent to the General Data Protection Regulation. All staff and volunteers, including contractors, sign confidentiality or non-disclosure agreements prior to being given access to confidential data.

We regularly review audit information for our main ICT systems to ensure that access to confidential data complies with our acceptable use policies. Any potentially suspicious activity is investigated and remedial actions taken where necessary – which may include retraining or disciplinary proceedings.

We implement a 'whistleblowing policy' which allows any staff member or volunteer to raise concerns about information risks, anonymously if necessary, so that these can be investigated and steps taken to adequately address any legitimate matters.

We will implement appropriate contractual requirements relating to data protection and information security as required by our funders and partner organisations.

**Signed …….**
**Trustee Board of Oasis Church Chelmsford**

**Date……**