Privacy Policy

Proximity Church Safeguarding Website

This privacy policy is relevant to ‘App v.22.10.12.1530’ of the Proximity Church Safeguarding Website located at https://safeguarding.proximitychurch.co.uk/ (the website).

Connecting to the website

The connection to the website is secured with a certificated provided by Let’s Encrypt. This means information you send or get through the site is private (encrypted).

Signing up

An account is required for every person who needs to record a concern, even if you intend to record the concern anonymously. The details we store on sign up include first name, last name, email address and the date-time of when the information was submitted and stored in the database. An account ID (user ID) and username are automatically and randomly generated, not based on any information you submit. This information is stored in plain text in the database. To activate the account, you will need to set a password, which is encrypted in the database. We store the date-time your account is activated.

Signing in

For every sign in attempt to the website (pressing submit when the email address and password fields contain text), we store the following information in the database, all in plain text. The date-time of the sign in attempt, the email address that was submitted, the users ID (if the email address finds a record in the database), the IP address the request came from (which looks something like “192.168.2.1”), the browser’s user agent (which looks something like, “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36”), and a note to say if the sign in was successful, or if not, why not.

Recording a concern

You can either record a ‘child’ or ‘adult’ concern on the website. The data submitted for a concern will be associated to your user ID, so we know it was you who raised the concern. You can only choose to record anonymously only for an ‘adult’ concern. If you record anonymously, the record of the concern in the database will not be associated to your user ID. The information collected differs for an ‘adult’ concern and a ‘child’ concern, as outlined below.

Starting to record a concern

You will need to read the disclaimer before you can record a concern. We will store if you start a child or adult concern. This information is displayed on your dashboard. You can delete concerns that you start, or you can choose to continue with the concern.

Recording an Adult concern

For each adult concern successfully submitted (confirmation message displayed on screen when successful), we store the following information in the database. Your user ID is associated to the record, unless you choose to record anonymously, in which case a NULL value is stored. Unique IDs are automatically and randomly generated.

The required information we store for an adult concern is the first name of adult, last name of adult, cause(s) for concern, concern summary, detailed account of what happened, action taken, concern date, and location of concern/incident.

The optional information we store is your telephone number, the telephone number of the adult this concern relates to, email address of the adult this concern relates to, address of the adult this concern relates to, and or a single file attachment.

Any plain text inputs are encrypted in the database record and not stored as plain text. Only functions built into the website can decrypt the encrypted data from the database.

Recording a Child concern

For each child concern successfully submitted (confirmation message displayed on screen when successful), we store the following information in the database. Your user ID is associated to the record. You cannot report anonymously for a child concern. Unique IDs are automatically and randomly generated.

The required information we store for a child concern is the first name of child, last name of child, cause(s) for concern, concern summary, detailed account of what happened, action taken, concern date, and location of concern/incident.

The optional information we store is your telephone number, child's date of birth, address of the child this concern relates to, parent or guardians first name, parent or guardians last name, parent or guardians telephone number, parent or guardians email address, if the child has an Education Healthcare Plan (EHCP) and or a single file attachment. Read below about the storage of file attachments.

Any plain text inputs are encrypted in the database record and not stored as plain text. Only the website can decrypt the encrypted data from the database.

Editing concerns and other data

Only the user who raised the concern can edit it, and it can only be edited within the first 30 minutes after submission. If any edits are successfully submitted, a notification email will be sent to the DSL.

Editing data in any form will overwrite previously submitted values in the database. There is no version control of data submitted.

Additional comments linked to a concern

If more information is required for a concern, a single text field is available to add that information. Information submitted will be encrypted in the database. These comments can only be edited within the first 30 minutes after submission by the user who submitted the comment, and cannot be deleted by any account.

Assessment of the concern

Only DSL accounts will be able to add assessments to concerns. A notification email will be sent to the person who raised the concern (if not anonymous) and to the other DSL accounts when the assessment is submitted. Information submitted will be encrypted in the database. These assessment can only be edited within the first 30 minutes after submission by the user who submitted the assessment, and cannot be deleted by any account.

Viewing concerns

On your dashboard, you will only be able to view concerns you have recorded. Only DSL accounts will be able to view concerns raised by all and any user.

Deleting data

Any data submitted by any user cannot be deleted by any user using functions built into the website, except for user accounts (details below). Sign in attempts, recorded concerns, additional comments of concerns, and assessments of concerns cannot be deleted.

Deleting user accounts

If a user's account is no longer required, it can be deleted by a DSL account using functions built into the website. If a user account is deleted, you will be able to create another account with the same email address if needed. By deleting the user's account, concerns recorded, additional comments added by that user and related assessments will not be deleted. Sign in attempt data linked to that account will not be deleted. The user's record will not be removed, but the email address will be replaced with random text. The first name and last name of that user's account will remain so the website can still display the name of the person who submitted data. The user will not be able to sign into their account once it is deleted. If the user is signed in when the account is deleted, they will be signed out when they click on any link on the website. If you do create an account with the same email address, their data previously input will not be associated to it because data is associated by a user's ID and not an email address.

Notification emails

Notification emails are sent to users and DSL accounts when new concern data is submitted or edited. The email will be sent from the account that submitted the concern data, meaning your first name, last name, and email address on your account at the time of submitting concern data will show as the 'from' field in the recipients email client. If you chose to submit anonymously, the notification email will be sent from a no-reply email account, so it cannot be linked to you. If a user submitted a concern anonymously, that user will not receive email notifications when further information is added to a concern. No personally identifiable information (PII) is stored in the body emails, except for a greeting name, and a web link to view the record on the website.

Concern attachments.

Only PDF and ZIP file types are accepted at a maximum of 9 MB. The file is uploaded to a dedicated directory on the Proximity Church Safeguarding subdomain and the file is renamed to a unique file name before it is stored in that directory. The original file name is encrypted in the database. You will not be able to view a list of files in this dedicated directory for storing files.