(3) Регистърът съдържа следните групи данни:

(а) име, ЕГН/ЛНЧ, адрес, телефони за връзка и месторабота;

(б) данни за родителски права и родствени връзки;

(в) телефонен номер, актуален имейл адрес и постоянен/настоящ адрес;

(г) образование и трудова заетост-по преценка на лицето.

(4) Нормативното основание – ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(5) Технологично описание на регистър „**Родители**“. Носители на данни:

(а) когато са на хартиен носител, данните се набират в писмена форма и се съхраняват в папки;

Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни, снабдени със заключващ механизъм.

(б) на технически носител: наличие на електронен дневник на всяки клас;

(в) срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(6) Определяне на длъжностите: обработващи лични данни на регистър **„Родители“** са: Директор, учители, зам.-директор УД, РУ, психолози, логопеди и сензорни терапевти.

(7) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(8) Организационни мерки за физическа защита: определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(9) Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми,