|  |  |
| --- | --- |
| **DATA PROTECTION BREACH**  **RISK ASSESSMENT** | Preston Hedge’s Academy Trust |

|  |  |  |  |
| --- | --- | --- | --- |
| **HAZARD** | **RISK**  **(WHAT HARM MIGHT BE CAUSED)** | **CONTROL MEASURES** | **RISK RATING AFTER CONTROL MEASURES** |
| Failure to notify the data subject of the processing of their information | Distress to the individual | * Privacy Notices, Information Audit, Data Protection Policy (needs to be clear and concise) * Effective publication 9of the above), using a range of media * Statements informing individual of the legal basis for the collection and processing of information * Clear expectations for the processing of data (including third party contracts) * A DPO for advice and guidance | Low |
| The data subject being unaware of the disclosure of information to another organisation or person | Distress to the individual and/or other persons | * Staff training * Privacy Notices, Information Audit, Data Protection Policy * Effective publication of the above), using a range of media * Statements informing individual of the legal basis for the collection and processing of information * Clear expectations for the processing of data (including third party contracts) * Effective process (e.g. double checks) to reduce the risk of disclosure in error * Clear lines of responsibility for processing operations | Low |
| Disclosure in error by email or electronic transfer and storage of files | Distress to the individual and/or other persons  Reputational damage and fines | * Minimise personal information transferred electronically between members of staff, governors etc. * Secure storage with controlled access * Encrypted files (password protected) * Double checks in place when sending emails to mass audience (e.g. reply to all) * Use of cloud based systems with password access, rather than locally stored devices * Deleting data that is no longer relevant (and not legally justifiable) * Contracts with third parties, specifying the length of time that data will be held | Low |
| Disclosure and loss of paper files | Distress to the individual and/or other persons  Reputational damage and fines | * Reduce the amount of paper files held by using technology as an alternative method of storage. * Where possible, upload paper files electronically, then shred * Shred or secure disposal of personal data that is no longer relevant (and not legally justifiable) * Files held in secure locations with controlled access * Minimise the need for duplicated information * Sign in and out system to know where and for how long information is located away from the school * Where possible, transfer of pupil information electronically and securely * Transfer of paper files securely (person to person, secure postal system) | Low |
| Loss or theft of physical devices or paper files | Distress to the individual and/or other persons  Reputational damage and fines | * Staff training * Minimise need for taking paper and devices away from the premises * Ensure staff do not leave devices and paper files in cars * Encrypt devices, and/or use secure cloud storage systems * Do not use generic passwords * Use electronic communication methods to parents i.e. data collection sheets * If transferring data collection sheets by paper, ensure parents are aware of the procedure and date of transfer * Where possible, transfer of pupil information electronically and securely * Signing out (or in) procedure of pupil paper files * Agreed protocols of disposal of personal information with third parties (e.g. for serious case reviews) * Personal information can be identified (so as not to get mislaid with other non personal documents) * Termination of employment meeting, signing of and hand over of equipment and personal information relating to the school community | Low |
| Unauthorised access |  | * Individual passwords on photocopiers, computers, cloud access, email access, personal storage devices * Employ IT specialist or company * Encrypted software systems (to minimise hacking) * Secure premises and signing in and out procedures * Clear desk policy and devices that close a period of stay idle * Staff training * Awareness of visitor zones (like parents evening or performances) or not visitor access to offices where personal information is stored * Limit access to electronic file that contain personal information * Procedures in place to secure the site outside of the school day * Procedure in place to ensure people no longer work for the school no longer have access to personal data. * Minimise the use of personal emails * Use email addresses attached to one individual (i.e. not family members) * Ensure personal information is erased on equipment that has to be returned at the end of a contract (ensure the contract states that the contractor will erase the information, if the school does not have the expertise to do so). | Low |
| Off-Site Visits |  | * Use electronic systems (i.e. Plumsun app), rather than using paper information * Where paper copies are issues, they should be signed out by individual members of staff and signed in at the end of the visit | Low |
| Future/ Potential Breaches |  | * Ensure a data impact assessment is completed for all new procedures or the purchase of new equipment * Ensure a procedure is in place to ensure the request of information is being made by a legitimate source – real and authorised person who will receive the information (i.e. when a pupil becomes 13 years old, then the parent does not have the right to request their siblings information or a parent who has separated they may request information that they are not legally allowed access to – careful of requests for fishing!) | Low |