



GDPR BREACH RISK ASSESSMENT		 
ASSESSMENT CARRIED OUT BY Emma Howard & Shaun Carter	DATE October 2021	

HAZARD	RISK  (WHAT HARM MIGHT BE CAUSED)	INITIAL RISK RATING	CONTROL MEASURES	FINAL RISK RATING
Failure to notify the data subject of the processing of their information	Distress to the individual	Medium	<ul style="list-style-type: none"> <li>Privacy Notices, Information Audit, Data Protection Policy (needs to be clear and concise)</li> <li>Effective publication of the above), using a range of media</li> <li>Statements informing individual of the legal basis for the collection and processing of information</li> <li>Clear expectations for the processing of data (including third party contracts)</li> <li>A DPO for advice and guidance</li> </ul>	Low
The data subject being unaware of the disclosure of information to another organisation or person	Distress to the individual and/or other persons	Medium	<ul style="list-style-type: none"> <li>Staff training</li> <li>Privacy Notices, Information Audit, Data Protection Policy</li> <li>Effective publication (of the above), using a range of media</li> <li>Statements informing individual of the legal basis for the collection and processing of information</li> <li>Clear expectations for the processing of data (including third party contracts)</li> <li>Effective process (e.g. double checks) to reduce the risk of disclosure in error</li> <li>Clear lines of responsibility for processing operations</li> </ul>	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	Medium	<ul style="list-style-type: none"> <li>Minimise personal information transferred electronically between members of staff, governors etc.</li> <li>Secure storage with controlled access</li> <li>Encrypted files (password protected)</li> <li>Double checks in place when sending emails to mass audience (e.g. reply to all)</li> <li>Use of cloud based systems with password access, rather than locally stored devices</li> <li>Deleting data that is no longer relevant (and not legally justifiable)</li> <li>Contracts with third parties, specifying the length of time that data will be held</li> </ul>	Low
Disclosure and loss of paper files	Distress to the individual and/or other persons  Reputational damage and fines	Medium	<ul style="list-style-type: none"> <li>Reduce the amount of paper files held by using technology as an alternative method of storage.</li> <li>Where possible, upload paper files electronically, then shred</li> <li>Shred or secure disposal of personal data that is no longer relevant (and not legally justifiable)</li> <li>Files held in secure locations with controlled access</li> <li>Minimise the need for duplicated information</li> <li>Sign in and out system to know where and for how long information is located away from the school</li> <li>Where possible, transfer of pupil information electronically and securely</li> <li>Transfer of paper files securely (person to person, secure postal system)</li> </ul>	Low
Loss or theft of physical devices or paper files	Distress to the individual and/or other persons  Reputational damage and fines	Medium	<ul style="list-style-type: none"> <li>Staff training</li> <li>Minimise need for taking paper and devices away from the premises</li> <li>Ensure staff do not leave devices and paper files in cars</li> <li>Encrypt devices, and/or use secure cloud storage systems</li> <li>Do not use generic passwords</li> <li>Use electronic communication methods to parents i.e. data collection sheets</li> <li>If transferring data collection sheets by paper, ensure parents are aware of the procedure and date of transfer</li> <li>Where possible, transfer of pupil information electronically and</li> </ul>	Low

			securely <ul style="list-style-type: none"> <li>• Signing out (or in) procedure of pupil paper files</li> <li>• Agreed protocols of disposal of personal information with third parties (e.g. for serious case reviews)</li> <li>• Personal information can be identified (so as not to get mislaid with other non personal documents)</li> <li>• Termination of employment meeting, signing of and hand over of equipment and personal information relating to the school community</li> </ul>	
Unauthorised access	Distress to the individual and/or other persons  Reputational damage and fines	Medium	<ul style="list-style-type: none"> <li>• Individual passwords on photocopiers, computers, cloud access, email access, personal storage devices</li> <li>• Employ IT specialist or company</li> <li>• Encrypted software systems (to minimise hacking)</li> <li>• Secure premises and signing in and out procedures</li> <li>• Clear desk policy and devices that close a period of stay idle</li> <li>• Staff training</li> <li>• Awareness of visitor zones (like parents evening or performances) or not visitor access to offices where personal information is stored</li> <li>• Limit access to electronic file that contain personal information</li> <li>• Procedures in place to secure the site outside of the school day</li> <li>• Procedure in place to ensure people no longer work for the school no longer have access to personal data.</li> <li>• All electronic communication for school business by staff through The Bliss Charity School email addresses.</li> <li>• Use email addresses attached to one individual (i.e. not family members)</li> <li>• 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).</li> </ul>	Low

Loss or theft of personal/sensitive data during off-site visits	Distress to the individual and/or other persons  Reputational damage and fines	Medium	<ul style="list-style-type: none"> <li>• Use electronic systems (i.e. Plumsun app), rather than using paper information</li> <li>• Where paper copies are issues, they should be signed out by individual members of staff and signed in at the end of the visit</li> </ul>	Low
Future/ Potential Breaches	Distress to the individual and/or other persons  Reputational damage and fines	Medium	<ul style="list-style-type: none"> <li>• Ensure a data impact assessment is completed for all new procedures or the purchase of new equipment</li> <li>• 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 phishing!)</li> </ul>	Low