QUESTION	RESPONSE
Roles and awareness of data protection in the School	
1) Which employees have specific roles in overseeing or managing data protection matters?	SBM, Admin team,
2) How aware are other individuals (staff, parents, children) of data protection. Are those individuals trained or made aware of data protection rights and the GDPR? If so how are they informed?	Staff meeting – training Website Staff bulletin Newsletters to parents
3) Has the School received any subject access requests in the last 3 years? Does the School keep a log of these requests?	Yes 4 Subject Access in GDPR file on Google drive HR file
4) Do individuals know who to contact about data protection in the School? If so, how?	Website
Policies and procedures	
5) What policies and procedures are in place covering data protection and related issues?	DP Policy, Staff Privacy Notice, Pupil Privacy Notice, CCTV Policy

6) Are these policies reviewed on a regular basis? If so, please detail how often they are reviewed.	Bi-annually as per FGP annual calendar 28.3.18, 06.06.19, 24.09.2020
7) Have these policies been updated in line with the GDPR?	Yes
8) How are policies made available to individuals (staff, parents)?	Website
9) Does the School have a record that employees have access to those policies and that they have read and understood them?	EVERY
Contracts of Employment	
10) Does the School have a clause on data protection within its employment contracts?	No but part of school's induction process
Reviews and assessments of data and privacy notices	
11) Does the School carry out privacy impact assessments or risk assessments when using new technologies or new services which impact on processing data?	Yes
12) If so, does the School record these assessments? Where?	In GDPR file on Google Drive
13) If so, does the School review these risk assessments to ensure compliance?	Yes annually
14) Does the School have privacy notices?	Yes
15) If so, where are they displayed/how are they given to individuals?	Website, annually with staff and induction with new staff

16) Do you have different privacy notices for different categories of individuals?	Staff and Pupils
17) Are the notices updated to reflect GDPR?	Yes
Training	
18) Has any data protection training taken place with staff?	Yes
19) Is this recorded/evidenced?	Staff meeting file
20) Have the designated data protection contacts within the School (and management who have responsibilities for data protection) received specific training on data protection?	Yes
21) Is this recorded/evidenced?	Educare level 2
Personnel Files	
22) How are personnel files kept?	Locked filing cabinets, currently being transferred onto Google drive but with only key personnel having access.
23) What electronic records are kept and how are they kept?	HR Google drive – authorised access
24) Who is authorised to view each record?	Authorised staff
25) Are those files reviewed regularly to ensure the record is up to date (and doesn't contain any unnecessary content)?	Every 6 months spot check. Action to check if confidentiality sheet is in all personnel files – MB/CA to check –These are all in place. All new starters complete these.
Emails	
26) Who is your email provider?	Google GSuite

27) Have their systems been updated with GDPR in mind?	Yes
28) How are your emails stored and backed up (if at all)?	Emails are all stored on Google Servers. These servers are located in Dublin, Ireland. Emails, Calendar, Contacts & Drive are backed up to Datto SAAS Protection, which stores its data within the UK.
29) Do you have a retention procedure for deleting emails?	No – (Jamie can set up so email delete after a certain amount of time – this to be agreed by h/t) Staff must not use their email site as a filing system and must move confidential documents to a different platform.
Data Breaches and Reporting	
30) Does the School have procedures in place for notifying of breaches of data protection?	Yes
31) Are staff aware of what a data breach is?	All staff have completed Educare
32) Have there been any known data breaches or matters that have been referred to the ICO? Have a log been taken of these breaches?	No
Reasons for Processing	
33) Are you, and the School as a whole, aware of the data protection principles and how they are supposed to be applied?	Yes
34) Is personal data and special categories of data processed by the School in accordance with the data protection principles?	Yes – GDPR Risk Assessment, 3rd Parties show GDPR Compliance
35) Are you, and the School as a whole, aware of the fair processing conditions and how they apply?	Yes – GDPR Website

36) Is personal data and special categories of data processed by the School in accordance with the fair processing conditions?	Yes
37) Are the reasons for processing data documented? If so where?	Detailed in GDPR file
38) Are you aware of any personal data being transferred outside of the EEA?	No – however we would have personal consent
Data Sharing With Third Parties	
39) Are you aware of whether the School shares data with third party organisations (either obtaining data from or data being passed to third parties)?	The school uses Wonde to sync ScholarPack data with School Spider, Times Tables Rockstars and iPAL, Education City, GL Assessment, IDL, Oxford Owl, Active Learn, Renaissance Learning, SeeSaw & Spelling Shed. ParentPay & SAM People use a secure API to directly export ScholarPack data. Hi-impact technicians have access to all data stored on school servers. The school has hi-impact remote support software installed on most school computers. The school has cloud backup to Redstor that stores server and SIMS data.
40) Do the school keep a record of these organisations? If so where are they kept?	Yes GDPR audit spreadsheet – compliance records
41) How are these arrangements monitored? Are there contracts in place with those third parties that cover data protection and security?	Yes compliance records
42) Have those agreements been updated to reflect GDPR requirements?	Yes
Security	

43) What security measures are there for storing and using paper records? And how are these security measures used?	Locked filing cabinets. Personnel records are in the process of being transferred onto shared drive then paperwork will be disposed of via confidential waste.
44) What security measures are there for storing and using electronic records? And how are these security measures used?	5-minute screen lock for all Office and SMT Staff. Password complexity requirements in place.
45) What steps are taken to ensure the effectiveness of any security measures in place (for example changing passwords, back-ups)?	School has 2 backups that are completed daily, one to a local encrypted drive and one to the cloud using Redstor. There is also a half termly backup to an external hard drive that is kept in the safe. Passwords must be at least 8 characters, can't be one you have used within the last 24 password resets, must contain a capital and a number and must be changed every 30 days.
46) Does the School use cookies? If so, does the School have a notice for cookies?	Website uses cookies and the cookie policy is on our website
Record Retention and Disposal	
47) Does the School dispose of data and records when no longer necessary?	In compliance with retention records policy
48) Are CCTV Records Disposed of in accordance with your CCTV Policy?	Yes automatically after 28 days
49) Does the School have a retention policy?	Yes adopts IRO
50) Are there secure methods for disposing and archiving items	Authorised shredding company
Portable Media Devices	
51) Does the School issue portable media devices?	Yes – Laptops and iPads

52) How are they issued?	Laptops are assigned to classrooms and iPads to class teachers.
53) What security is in place to protect them and restrict their use	Teacher iPads are required to be passcode protected. Laptop user accounts are password protected complying with the password complexity rules and all local offline files are encrypted.