DOWNTON PRIMARY SCHOOL

Data Protection in Practice Document

February 2019

This guidance should be read and understood in conjunction with the following policies and guidance:

- The Data Protection Act 1998 in readiness for May 2018.
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2015
- Data Protection Policy 2018
- Retention Policy
- Acceptable use policy
- Retention Policy
- Data Protection Procedures May 2018
- Governors and staff code of conduct.
- E Safety Policy
- Confidentiality Agreement
- Whistle Blowing Policy
- Keeping Children Safe in Education 2016
- Guidance for Safer Working Practice for those working with children and young people in education settings October 2015
- The Prevent Duty June 2015
- Guidelines for Schools on Record Keeping and Management of Child Welfare and Child Protection Information Wiltshire Council Feb 2017
- Becta: Information Risk Management and Protective Marking
- Records Management Society – Tool Kit for Schools

The 8 Principles are below and how they are being implemented in school.

Principle	Definition	In Practice
1. Be processed fairly and lawfully	A. have legitimate grounds for collecting and using the personal data; B. not use the data in ways that have unjustified adverse effects on the individuals concerned; C. be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data; D. handle people's personal data only in ways they would reasonably expect; and E. make sure you do not do anything unlawful with the data.	• Contact information for emergencies • Census • Pay and contracts for staff • DBS • Health and medical needs • Helping to track pupils attainment and progress throughout the school • Attendance • SEN information • Safeguarding and Child protection • Business interests of Governors and Staff stored securely. This data would need to be shared with any necessary agencies and the council. All this data will be stored securely within school and on encrypted devices or the school server. If there has been a data breach then staff and governors need to report the breach using the data breach form. This form is then given to the Data Protection Controllers at Greentrees Primary School. The data Protection Controllers are Mrs Paula Carlton, Head teacher and Mrs Susan Foyle, School Finance Officer. They will then determine if a serious breach has occurred. If this proves to be the case then the breach is referred to the Data Protection Officer, Mr Wes Thorpe, Head of Alderbury and West Grimstead School, who will determine if the breach needs to be referred to the Information Commissioner Officer (ICO).

2. Be collected for a specified purpose and not used for anything incompatible with that purpose	A. be clear from the outset about why you are collecting personal data and what you intend to do with it; B. comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data; C. comply with what the Act says about notifying the Information Commissioner; and D. ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.	• See above • This data would need to be shared with any necessary agencies and the council. • Ensure that pictures for the website, around the school and Facebook, have prior consent from both pupils and staff. • Notices to parents at shows, sports days and external events must ensure that the school give prior warning about pictures being publicly used. • Standard template notification notice to be used. • Ensure school is registered with the ICO yearly. • For safeguarding it would be fair to disclose the information to other agencies without prior consent.
3. Be adequate, relevant and not excessive	A. you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and B. you do not hold more information than you need for that purpose.	• Personal data will only be stored on SIMS and securely in the office. • Learners of the Week will be on display with child's first name and surname. • Any school councillors will only have a picture and first name. On the website it will only be a picture (with prior agreement with parents). • Medical equipment will be labelled with child's name. • Medical folder with child's Full name and picture will be stored centrally in a locked cabinet and made available to employees when required. • No other information will be displayed around the school with personal information unless for safeguarding

		reasons. • Emailed data must be password protected and not printed.
4. Be accurate and up-to-date	A. take reasonable steps to ensure the accuracy of any personal data you obtain; B. ensure that the source of any personal data is clear; C. carefully consider any challenges to the accuracy of information; D. consider whether it is necessary to update the information.	• Use of the CAPITA SIMS App to obtain updated information from parents, Staff and Governors (or by coming into the school office and informing office staff there and then). • If children are put on or taken off agency records then any changes must be in writing and a record securely kept. • If a child, staff or Governor leave all emails from or to that individual must be cleared from records in line with the retention policy. • Only school email address to be used for correspondence. • Governors to use GVO to access information for Governors meetings.
5. Not be kept longer than necessary	A. review the length of time you keep personal data; B. consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it; C. securely delete information that is no longer needed for this purpose or these purposes; and D. update, archive or securely delete information if it goes out of date.	• When deleting information – it must be shredded with a cross shredder and not left on the side at any time. • Governors will ensure that all documents and correspondence are deleted in line with the Retention Policy. Any paper documents to be handed back to the school. • All these will be in line with the Retention Policy and Data Protection Policy 2019

6. Be processed in accordance with the rights of the data subject	A. a right of access to a copy of the information comprised in their personal data; B. a right to object to processing that is likely to cause or is causing damage or distress; C. a right to prevent processing for direct marketing; D. a right to object to decisions being taken by automated means; E. a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and F. a right to claim compensation for damages caused by a breach of the Act.	• A copy will be supplied as in the guidelines of the GDPR ACT 2018 (Except for Easter and Summer Holidays). This means you must be able to put on hands on every piece of evidence that you have of that child. This will be completed within 20 working days. • Signed consent will be sought before any marketing pictures are used. • Retention Policy and Data Protection Policy will be used to erase and destroy information. • See GDPR ACT 2018 for damages and breach of Act. • See Data Protection policy May 2018.
7. Be kept securely	A. design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach; B. be clear about who in your organisation is responsible for ensuring information security; C. make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and D. be ready to respond to any breach of security swiftly and effectively.	• All employees to have a passcode to the printer and must be at the printer for secure information. • All sensitive information to be locked in lockable cabinets. • All sensitive information to be stored on encrypted school devices. • Computer must be 'locked' or logged off when the user is not in the room. • Employees must use a password and not share this with any other person. • No personal devices used by employees to access secure data including emails unless password or fingerprint identification protected. No e-mail pop ups on personal phones allowed. • All data and letters about children to be stored in their personal folder or on the secure data drive.

		• IT devices to be securely closed down when employees step away form the device. • Employees to only use school server or encrypted device when working at home. • Children's work books to be stored securely when being transported to and from school. No children's workbooks to be left unattended in unlocked cars. • All staff files to be stored in a lockable cabinet. • Once training has been completed and policy read all staff are responsible for ensuring information is secured. • Follow GDPR policy and Retention Policy May 2018 for a breach and ICO recommendations for a breach. • If using own device to complete school work then staff and Governors must follow the Acceptable use policy. • Staff and Governor signing in and out sheet kept securely. • Pupil signing in and out book kept securely.
8. Not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.	A Consider if you need to transfer personal data abroad. B Determine if you are transferring the data to a country outside the EEA or will it just be in transit through a non-EEA country. C Comply with all the other data protection principles D Determine if the transfer is to a country on the EU Commission's list of countries or territories providing adequate protection for the rights and freedoms of data	• These are only relevant for pupils moving outside of the UK. • When sharing information with link schools abroad all the data protection advice above applies.

	subjects in connection with the processing of their personal data. E Decide if the transfer is to the United States of America, has the US recipient of the data provided adequate protection for the transfer of personal data.	