BANTOCK PRIMARY SCHOOL

Data Protection Policy

Headteacher	**H Sarai**
Chair	**N Round**
Approved Date	**27.09.18/04.12.19/2.12.20**

CONTENTS

1 INTRODUCTION

1.1 Bantock Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.

1.2 School staff are obliged to comply with this Policy when processing Personal Data on the school's behalf. Any breach of this Policy by school staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

2.1 The school holds Personal Data about current, past and prospective pupils, parents, employees and others with whom the school communicates. Personal Data may be recorded on paper, stored electronically, visual media or other formats.

2.2 This Policy and other documents referred to in it set out the basis on which the school will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Officer is responsible for supporting the school with compliance with the Relevant Data Protection Laws and with this Policy. That post is held by Services4Schools Ltd. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer. The Data Protection Officer can be contacted at DPO@bantockprimaryschool.co.uk

3 DEFINITION OF DATA PROTECTION TERMS

3.1 In this Policy, the functions of the school are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the school 'carrying out its functions' or similar are references to these activities.

3.2 References to 'we' are references to the school.

3.3 **Data Subjects** means identified or identifiable natural (living) persons whose Personal Data the school holds. These may be pupils, parents/carers, staff, governors, visitors etc. This Policy also refers to Data Subjects as 'individuals.'

3.4 **Data Controllers** are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing. The school is the Data Controller of all Personal Data used for carrying out its functions.

3.5 **School Staff** are, for the purposes of this Policy, those of our employees whose work involves processing Personal Data. School staff must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

3.6 **Data Processors** include any person or organisation, who is not a member of school staff, which processes Personal Data on the school's behalf, including any external suppliers that handle Personal Data on the school's behalf.

3.7 **Privacy Notices** are documents explaining to Data Subjects how their data will be used by the school.

3.8 **Personal Data** means any information relating to an identified or identifiable natural (living) person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.9 **Personal Data Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data the school is responsible for.

3.10 **Pseudonymisation** means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information. This additional information (or key) must be kept separately and is subject to measures to ensure that the identity of the Data Subject remains protected.

3.11 **Relevant Data Protection Law** means the Data Protection Act 2018, the General Data Protection Regulation ((EU) 2016/679), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

3.12 **Special Categories of Personal Data** (formerly known as 'sensitive Personal Data') includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data for, or on behalf of, the school must comply with the principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:

4.1.1 processed fairly, lawfully and transparently;

4.1.2 processed for specified, limited and legitimate purposes and in an appropriate way;

4.1.3 adequate, relevant and not excessive for the purposes for which they are processed;

4.1.4 accurate and, where necessary, kept up to date;

4.1.5 not kept longer than necessary for the intended purpose of processing; and

4.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The school will keep a record of all Data Processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:

5.1.1 the individual's explicit consent to the processing for one or more specified purposes;

5.1.2 that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the school is subject;

5.1.3 that the processing is in the public interest; or

5.1.4 that the processing is in the legitimate interest of the school or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.

5.2 Where a change to a process, or introduction of a new process involving the use of large volumes of Data Processing, that is likely to pose a high risk to individuals' rights, the school will carry out an appropriate Privacy Impact Assessment.

5.3 *Special Categories of Personal Data*

5.4 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

5.4.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the school or of the individual in the field of employment and social security and social protection law;

5.4.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;

5.4.3 relates to Personal Data which are manifestly made public by the individual;

5.4.4 is necessary for reasons of substantial public interest; or

5.4.5 is necessary to protect the vital interests of the individual.

5.5 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK or EU law states that processing must take place.

5.5.1 This is undertaken as part of the pre-employment check process (DBS) for all staff employed by the school, or where it is necessary to perform such a check as required by safeguarding regulation.

5.6 *Consent of adults and organisations*

5.7 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the school) or a positive action demonstrating consent. Any requests that the school makes for consent must be in clear language.

5.8 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the school requests consent.

5.9 *Consent of children and young people*

5.10 Parental consent to Data Processing must be obtained for pupils or other children younger than 16 years of age.

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

6.1 In the course of carrying out its functions, the school may collect and process the Personal Data set out in its data asset register. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers, other schools, the local authority or other public bodies, recruitment agencies or service providers, professional advisers and others).

6.2 The school will only process Personal Data for the specific purposes set out in Information Asset Register or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject via Privacy Notices, or consent forms as appropriate.

6.3 CCTV is used by the school to support the prevention and deterrence of crime and to support pupil behaviour policies.

6.4 Where the use of CCTV include the recording of images of identifiable individuals, the school will comply with the Data Processing principles within this Policy.

6.5 The use of CCTV is to ensure the school site is secure. The school will adhere to the ICO's code of practice for the use of CCTV. All pupils, staff and visitors will be notified that CCTV is in operation via signage.

6.6 The school will ensure that all CCTV footage will be kept for up to 60 calendar days for security purposes before being deleted, unless subject to a criminal or internal investigation.

6.7 Any enquiries about CCTV systems across the school should be directed to the Headteacher in the first instance.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual.

7.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, he or she should notify the Data Protection Officer.

8 ACCURATE AND UP-TO-DATE DATA

8.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8.2 It is the responsibility of staff to ensure that Personal Data is accurate and kept up to date. All staff must as a minimum check that any Personal Data that they provide to the school in connection with their employment is accurate and up to date. They must also inform the school of any changes to their Personal Data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

9 TIMELY PROCESSING

9.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. We will be guided by the Information Records Management Society guidance in respect of decision making concerning the retention of Personal Data (Schools Toolkit 2016).

9.2 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, he or she should notify the Data Protection Officer.

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

10.1 We are committed to upholding the rights of individuals to access Personal Data the school holds on them.

10.2 We will process all Personal Data in line with individuals' rights, in particular their rights to:

10.2.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible

and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

10.2.2 receive confirmation as to whether your Personal Data is being processed by us;

10.2.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. School employees who receive a written request should forward it to their line managers and the Data Protection Officer immediately;

10.2.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the school (see also Paragraph 8);

10.2.5 restrict processing of data if one of the following circumstances applies:

a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;

b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

c) the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

d) the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

10.2.6 Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and the Data Subject shall be informed.

10.2.7 Where processing is restricted under one of the grounds in Paragraph 10.2.5, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom.

10.2.8 An individual who has obtained restriction of processing under Paragraph 10.2.5 shall be informed by the school before the restriction of processing is lifted.

10.2.9 Receive data concerning the individual, which he or she has provided to the school and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the school.

10.2.10 Object to Data Processing on grounds relating to his or her particular situation unless the school demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

10.2.11 Not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.

10.3 It is the responsibility of all staff to ensure that any request by an individual under Paragraph 10.1 is brought to the attention of the Data Protection Officer without undue delay.

10.4 The school may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

10.5 The school shall provide information on action taken on a request under Paragraph 10.1 to the individual within one month of receipt of the request unless the school deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

10.6 If a request under Paragraph 10.2 is unfounded or excessive, the school may charge a reasonable fee for providing the information or refuse the request.

10.7 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

10.7.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

10.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.8 Our employees will refer a request to the Headteacher and the Data Protection Officer. Employees should not be bullied into disclosing personal information.

11 NOTIFYING DATA SUBJECTS

11.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

11.1.1 the identity and contact details for the school and its Data Protection Officer;

11.1.2 the purpose or purposes for which we intend to process those Personal Data;

11.1.3 the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and

11.1.4 the means, if any, by which individuals can limit our use and sharing of their Personal Data.

11.2 If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Paragraph 11.1 above at the following times:

11.2.1 within one month of receiving the Personal Data;

11.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

11.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

11.3 A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

11.4 We will also inform individuals whose Personal Data we process that the school is the Data Controller with regard to those data and who the Data Protection Officer is.

12 DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures.

12.3 School staff will be issued with details of their obligations in relation to security of Personal Data.

12.4 All school staff must:

12.4.1 assist the school in upholding individuals' Data Protection rights;

12.4.2 only act in accordance with the school's instructions and authorisation;

12.4.3 notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Paragraph 12.5;

12.4.4 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

12.4.5 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.4.

12.5 The school will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.

12.6 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.6.1 **Confidentiality:** only people who are authorised to use the data can access them;

12.6.2 **Integrity:** Personal Data should be accurate and suitable for the purpose for which they are processed;

12.6.3 **Availability:** authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the school's central computer system instead of on individual computers, tablets or other media.

12.7 Security procedures include:

12.7.1 **IT Equipment:** Staff must ensure they have read the school's ICT policy before using school equipment, individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended.

12.7.2 **Building Security and Entry controls:** All visitors are required to sign in using appropriate systems. Any unauthorised person seen on the school's premises should be reported.

12.7.3 **Secure lockable storage:** Rooms, desks, cupboards and filing cabinets should be kept locked when unattended if they hold confidential information of any kind (personal information is always considered confidential).

12.7.4 **Appropriate Sharing and Verbal Disclosure:** When providing personal information verbally, particularly by telephone, it is most important that the individual's identity is verified before any information is disclosed and that conversations occur in a space where information cannot be overheard.

12.7.5 **Methods of disposal:** Paper documents containing personal information should be

shredded when they are no longer needed. Digital storage devices should be handed into relevant staff at the school to be securely destroyed when they are no longer required.

12.7.6 **Personal Data on display:** All Personal Data displayed in the school's buildings will be limited to what is necessary and pseudonymised where appropriate. If Personal Data is displayed externally, then consent should be sought prior to publication.

12.7.7 **Electronic Transport/Transfer of Personal Data:** School staff will use only approved methods to transport or transfer data as detailed in the school's ICT policy.

12.7.8 **Photographs and Digital Images:** (including video). We use photographs and digital images for a variety of purposes across the school, these include, but are not limited to:

- Capturing development and progress in learning
- School prospectuses and other publications focussed on promoting the school
- Assemblies and celebration events
- Sports day
- School performances
- Social Media
- Trips and residential outings

12.8 Where images of children or staff are used in public areas or made available online via publication on the school's website, the school will always seek consent before images are published.

12.9 The school shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement Data Protection principles and to integrate the necessary safeguards into processing activities.

12.10 The school shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 REGISTER OF PROCESSING ACTIVITIES

13.1 The school must maintain an accurate and up-to-date Information Asset Register of processing activities carried out by the school.

13.2 The school must record the following information for each processing activity:

13.2.1 the contact details for the school and its Data Protection Officer;

13.2.2 the purpose or purposes for which the processing activity has occurred;

13.2.3 descriptions of the categories of individuals involved in the processing activity;

13.2.4 descriptions of the categories of Personal Data involved in the processing activity;

13.2.5 descriptions of the categories of recipients of the Personal Data involved in the processing activity;

13.2.6 details of any transfers to third parties, including documentation of the transfer mechanism safeguards in place;

13.2.7 retention schedules;

13.2.8 descriptions of technical and organisational security measures in place relating to the processing activity.

13.3 It is the responsibility of all staff, to notify the Data Protection Officer of any changes that affect the use of Personal Data to ensure that the register of processing activities is accurate and kept up to date.

14 REGISTER OF BREACHES

14.1 The school must maintain an accurate and up-to-date register of all Personal Data Breaches.

14.2 If anyone becomes aware of a Data Protection breach they must inform the Data Protection Officer immediately. A plan for managing Data Breaches will be made available to all staff.

15 DATA PROTECTION OFFICER

15.1 The Data Protection Officer is responsible for supporting the school in compliance with Relevant Data Protection Law and with this Policy. The Data Protection Officer reports to the school's Headteacher and Management Committee, but fulfils their Data Protection functions independently.

15.2 The Data Protection Officer for the school is provided by Services4 Schools Ltd and can be contacted at DPO@bantockprimaryschool.co.uk or by writing to Bantock Primary School, Aston St, Pennfields, Wolverhampton WV3 0HY. Please address letters: **For the attention of the Data Protection Officer.**

15.3 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

15.4 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

16 USING DATA PROCESSORS

16.1 The school retains the right to engage by written contract any person or organisation, who is not a member of school staff, to process Personal Data on our behalf.

16.2 Data Processors must:

16.2.1 assist the school in upholding individuals' Data Protection rights;

16.2.2 only act in accordance with the school's instructions and authorisation;

16.2.3 maintain a written record of processing activities carried out on behalf of the school and provide this to the school within [a reasonable period] following request;

16.2.4 notify the school of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Paragraph 13;

16.2.5 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

16.2.6 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.4.

17 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1 Individuals have particular rights with regard to transfers of their Personal Data outside the European Economic Area ('EEA'). Circumstances in which the school may need to transfer data outside the EEA might include use of IT services hosted overseas, arrangement and administration of school trips and cultural exchange projects.

17.2 Subject to the requirements in Paragraph 12.1 above, Personal Data we hold may also be processed

by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

17.3 We may transfer any Personal Data we hold to a country outside the EEA provided that:

17.3.1 the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and

17.3.2 any transfer to a country or countries outside the EEA is subject the escalation procedure under Paragraph 17.4.

17.4 Before a transfer of Personal Data is made outside the EEA, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

17.4.1 confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country;

17.4.2 standard Data Protection Paragraphs adopted by the European Commission in accordance with Relevant Data Protection Law must be included in relevant documentation;

17.4.3 ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;

17.4.4 confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;

17.4.5 confirmation that the transfer is necessary for important reasons of public interest;

17.4.6 the Data Protection Officer must authorise the transfer.

18 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

18.1 We may share Personal Data we hold with staff within the school.

18.2 We may also disclose Personal Data we hold to third parties:

18.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

18.2.2 in order to enforce or apply any contract with the individual or other agreements; or

18.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

18.3 We may also share Personal Data we hold with selected third parties for the purposes set out in the school's Information Asset Register

19 REQUESTS FOR INFORMATION

19.1 Requests for information may take the following forms:

19.1.1 Requests for education records.

19.1.2 Freedom of information requests.

19.1.3 Subject access requests.

19.2 Where a person with parental responsibility requests information about a child's educational records, then advice should be sought from the Data Protection Officer.

19.3 If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. If a freedom of information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted.

19.4 If a person makes a subject access request, then they are requesting the personal information that the school has about them. There are exemptions to disclosing some information but these are more limited as a person has a right to know what information is held on them. If a subject access request is made, then the Data Protection Officer should be contacted immediately.

20 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. This Policy will be published on the school's website.

21 CORONAVIRUS – DATA PROTECTION ISSUES AND GUIDANCE ON WORKING FROM HOME

This information combines advice issued by the Information Commissioners Office and guidance produced by your Data Protection Officer. It aims to help you consider some of the additional risks, issues and mitigations that schools may face during the coming period.

21.1 **ICO Advice**

21.1.1 During the pandemic, we are worried that our data protection practices might not meet our usual standard or our response to information rights requests will be longer. Will the ICO take regulatory action against us?

No. We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period.

21.2.1.3 We can't extend statutory timescales, but we will tell people through our own communications channels that they may experience understandable delays when making information rights requests during the pandemic.

21.2 **Can I tell my staff that a colleague may have potentially contracted COVID-19?**

Yes. You should keep staff informed about cases in your organisation. Remember, you probably don't need to name individuals and you shouldn't provide more information than necessary. You have an obligation to ensure the health and safety of your employees, as well as a duty of care. Data protection doesn't prevent you doing this.

21.3 **Can I collect health data in relation to COVID-19 about employees or from visitors to my organisation? What about health information ahead of a conference, or an event?**

You have an obligation to protect your employees' health, but that doesn't necessarily mean you need to gather lots of information about them.

It's reasonable to ask people to tell you if they have visited a particular country, or are experiencing COVID-19 symptoms.

21.4 You could ask visitors to consider government advice before they decide to come. And you could advise staff to call 111 if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

If that's not enough and you still need to collect specific health data, don't collect more than you need and ensure that any information collected is treated with the appropriate safeguards.

21.5 **Can I share employees' health information to authorities for public health purposes?**

Yes. It's unlikely your organisation will have to share information with authorities about specific individuals, but if it is necessary then data protection law won't stop you from doing so.

21.6 **Working From Home or Away From School ICO Guidance**

More of our staff will be homeworking during the pandemic. What kind of security measures should my organisation have in place for homeworking during this period?

Data protection is not a barrier to increased and different types of homeworking. During the pandemic, staff may work from home more frequently than usual and they can use their own device or communications equipment. Data protection law doesn't prevent that, but you'll need to consider the same kinds of security measures for homeworking that you'd use in normal circumstances.

21.7 **Advice from your Data Protection Officer**

21.7.1 **Reporting Breaches and Issues**

If you are working from home, normal process for reporting data breaches still apply. Any issues relating to data protection or potential breaches should be reported to your Data Protection Officer (DPO), using the DPO email address set up by your school/Trust.

We will continue to monitor your DPO email address (or reporting systems) throughout any period of school closure.

21.8 **Working at home with paper records**

21.8.1 Where staff are required to take home school documents that contain significant amounts of personal data, such as those held by the central office or pupil records, it is recommended that the school retain a log of this transfer, signing records out when removed and back in once returned. This provides an audit trail and it will remind staff of their responsibility to prevent the documents from being lost or stolen (see accompanying record sign out procedure). See Appendix 21.8.1

21.9 Staff who are working from paper records and manual systems containing personal data, should take additional care in how information is stored at home.

21.9.1 Try to create a private working area so information is not exposed unnecessarily to other people at home.

21.9.2 Store records in safe areas - filing cabinets and lockable drawers cupboards are preferable, but otherwise, store files in boxes or bags that can be put away out of sight when not in use.

21.9.3 Leave papers and documents stored away until you need to work with them and after you have finished working, return all documents to your storage space.

21.9.4 Don't leave files and documents in cars or in bags that also contain laptops or mobile devices

21.10 **Using school IT equipment at home**

21.10.1 Store your equipment in a safe place at home. Do not leave laptops, mobile devices or other equipment out when not in use (e.g. overnight, at weekends)

21.10.2 Ensure that required school security standards are adhered to at all times - Don't share passwords to school equipment with family members, or other people at home. If you are not sure what your school/trust expects – check IT policies for details.

21.10.3 Avoid sharing devices among family or friends.

21.10.4 Don't leave laptops or other devices unattended. Lock your session (Windows Key + L on a windows laptop or close the case/ single short press of the power button on a mobile device)

21.10.5 When using equipment at home, be aware of what is visible on your screen and who else may be able to see this.

21.10.6 If using remote meeting software or video calls (Skype, Zoom, Teams, Facetime, etc) be mindful of your own privacy. Before joining a meeting/starting a call, plan ahead and advise your participants if it is not appropriate to discuss certain matters.

21.10.7 Check before you start the meeting that any documents you share online contain only information appropriate for sharing. If you are working with multiple documents, it may be necessary to close these before starting/joining an online meeting or call.

21.10.8 Be aware of your own privacy including personal photos or similar items that may be visible in the background when cameras on devices are used at home.

22.0 **Data Sharing – Personal Data**

22.1 Data protection does not prevent the sharing of personal data in emergency situations, as long this is approached in a sensible and proportionate way. You should, however, only share data where it is necessary and proportionate.

22.2 You may be required to share information quickly, especially with public health or government agencies. Data protection should not prevent this. Consider what is required and whether what you have been asked to share is proportionate - if something feels excessive from the public's point of view, then it probably is.

22.3 You may need to collect or share contact details you didn't need to before, such as email addresses, or other identifying information to support online learning system, or other emergency resources. In these instances, limit the information you need to collect or share to only what is required to complete your purpose.

22.4 If information has to be shared to enable the delivery of teaching and learning, you may not need additional consent as this may be justified through the 'performance of a public task' condition for processing.

22.5 Individuals should where possible be informed about what's happening to their data prior to it being used, as everyone still has a right to be informed about certain changes relating to the processing /sharing of their data.

23. **Records and Documents Sign In / Out Procedure & Register**

23.1 As far as possible, data should be in an electronic format on the server that can be accessed remotely.

23.2 Staff should ensure they follow the data protection guidance and ICT acceptable use agreement that include using devices. Devices should be password protected and locked when not in use.

23.3 For necessary physical records, staff should sign out the records and sign them back in once they have been returned.

23.4 These include records or documents with more substantial amounts of personal data that need more scrutiny in how they're handled.

These may include:

23.4.1 Pupil records

23.4.2 Attendance and assessment records

23.4.3 Safeguarding records

23.4.4 Annual or termly pupil reports

23.4.5 EYFS Profiles

23.4.6 Higher or further education references

24.0 Records or documents with little personal data, such as student work books or coursework, are suitably low risk and do not need to be recorded.

24.1 This procedure ensures school maintains a record of who holds particular records and documents at all times and when taken off site. It supports both school and staff with their responsibility to prevent the documents from being lost or stolen and supports data breach reporting.

24.2 The registers should be located in a relevant office or location with the member of staff assigned with the responsibility for the category of records.

24.3 Staff should keep documents in a secure file such as a closed folder or one with a zip lock. Staff should include their name and contact details in case the folder is lost.

24.4 Staff should keep documents in a secure place such as a secure area of their house, somewhere specific, such as a certain drawer or tray, to prevent them from being lost.

24.5 Staff should avoid leaving documents in their car as this creates a higher risk of them being stolen.

24.6 When returning the documents to school, staff should update the records register and take them immediately to their original storage place rather than leaving them on desks to return later.

24.7 If documents are copy documents that do not need to be returned to record set then confirmation of their destruction should be noted on the register.