



DATA PROTECTION POLICY including FREEDOM OF INFORMATION POLICY

The Richard Huish Trust

Trust Executive



Reviewed by Amy Britton, RHT Data Protection Officer

Approval date 6 July 2021

Next review date January 2024

This policy is based on the model policy produced eLim



Contents

	Page
1. Introduction	3
2. About this policy	3
3. Definition of data protection terms	3
4. Data Protection Officer	4
5. Responsibilities of the Trust and its Schools	4
6. Responsibilities of Staff, Governors and Volunteers	4
7. Informing parents/guardians and seeking consent	5
8. Rights of the data subject	6
9. Freedom of Information request policy	7
10. Data security	8
11. Data breaches	10
12. Data retention policy including emails	11
13. Reporting policy incidents	11
14. Monitoring and evaluation	11
15. Links to other policies	11
Appendix 1.1 Data protection terms and definitions	12
Appendix 1.2 Data protection principles	13
Appendix 1.3 Rights of the data subject and how we uphold them	14
Appendix 2 Role of the Data Protection Officer	16
Appendix 3 Role of the Data Protection Lead	18
Appendix 4 Privacy Impact Assessment	19
Appendix 5 Subject Access Request process	22
Appendix 6 Freedom of Information request process	24
Appendix 7 Data breach process	26

Contacts

RHT Data Protection Officer

Amy Britton

dposchools@somerset.gov.uk

Introduction

- 1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a school we will collect, store and process personal data about our pupils, staff, parents and others. This makes us a data controller in relation to that personal data.
- 1.2. We are committed to the protection of all personal data and special category personal data for which we are the data controller.
- 1.3. The law imposes significant fines and reputational penalties for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in penalties being applied.
- 1.4. All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.
- 1.4.1. This policy applies to all the schools in the Richard Huish Trust (The Trust):

The Taunton Academy
West Buckland Primary School & Nursery
North Curry C of E Primary School & Pre-School
North Town Primary School & Nursery
Nerrols Primary School & Nursery
Lyngford Park Primary School

About this policy

- 2.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce (including staff, volunteers and governors) and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'Data Protection legislation').
- 2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.
- 2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Definition of data protection terms

The Trust is registered as the **Data Controller** with the ICO. The Headteacher acts as a representative on a day-to-day basis. A list of definitions is included in **Appendix 1.1** to this policy.

Data Protection Officer

- 4.1 As a Trust we are required to appoint a Data Protection Officer (DPO - **see Appendix 2**). Our DPO is Amy Brittan and can be contacted at dposchools@somerset.gov.uk
- 4.2 The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. 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 DPO.
- 4.3 The DPO will provide the Trust with an annual report on compliance including reported data breaches, requested for information and other interactions with the Trust.
- 4.4 Other day to day matters will be dealt with by the school's Data Protection Lead (DPL - **see Appendix 3**), The Headteacher, Deputy Headteacher, and the Senior Administrator with the full support and guidance of the DPO.

Responsibilities of the Trust and its Schools

- 5.1 Richard Huish Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, students, parents and governors. The Trust and its schools will:
 - a) Follow the key principles of Data Protection legislation including the 6+1 principles of UK GDPR (**see Appendix 1.2**);
 - b) register with the Information Commissioners Office (ICO);
 - c) keep an up-to-date Data Asset Audit which lists all known uses of personal data in the school including the lawful basis for processing under Data Protection legislation, who it is shared with, where it is stored (including transfer out of the UK) and how long it is retained for.
 - d) verify that all systems that involve personal data or confidential information will be examined to see that they meet Data Protection regulations (**see paragraph 10 Data security**)
 - e) inform all users about their rights regarding data protection;
 - f) provide training to ensure that staff know their responsibilities;
 - g) monitor its data protection and information security processes on a regular basis, changing practices if necessary (**see paragraph 10 Data security**).

Responsibilities of Staff, Governors and Volunteers

- 6.1 All staff, governors and volunteers are responsible for checking that any information that they provide to the school or Trust is accurate and up to date.
- 6.2 All staff are responsible for ensuring that any personal data they use in the process of completing their role:
 - a) is not in the view of others who do not have the authority to view the data;
 - b) is kept securely in a locked cabinet when not being used;
 - c) is stored on a secure local or network drive;

- d) if on a school PC or laptop, that the device is locked when the staff member is out of the room;
 - e) that passwords for school systems are not shared with other staff members or students;
 - f) if kept on removable storage (laptop, tablet, USB memory stick) approved by the school, that this is password protected and encrypted. The data held on these devices must be backed up regularly and this is the responsibility of the individual;
 - g) is not disclosed to any unauthorised third party (this includes verbal disclosures of confidential information);
 - h) is assessed and approved by the Senior Leadership Team or the DPL with advice from the DPO (see **Appendix 4 Privacy Impact Assessment**) if used within an app, web service or other application.
- 6.3 Staff should follow the security measures set out in **paragraph 10 Data security**.
- 6.4 Staff will report any loss, theft or mishandling of personal data promptly to the data protection lead.
- 6.5 Staff should note that unauthorised disclosure or transgression of the above statements or security measures in may result in disciplinary or other action.
- 6.6 Staff and governors should ensure that they use the email address provided by the Trust for **only** school-related business and communication. All communication remains the property of the school and may be disclosed as part of a Subject Access Request (**see Appendix 5**)
- 6.7 If using a personal device to access school emails, the staff member / governor will take care not to download any personal information about students or other staff to their personal device, and respond to emails within the email app.
- 6.8 Staff and governors will follow the email retention policy as laid out in **paragraph 12 Data retention policy including emails**.
- 6.9 When staff and governors leave the school, they are required to hand over all personal data belonging to other pupils or staff. They must not remove any personal data without the permission of the school. Taking personal data with no lawful basis may be a criminal offence.

Informing parents/guardians and seeking consent

- 7.1 The school will inform the Parents/Guardians of the importance of the personal data the school uses and the importance of keeping this up to date. This process will include at least an annual data collection sheet (with the return of this document being recorded) and reminders to update personal information (e.g. contact numbers) in newsletters and at tutor or class meetings.
- 7.2 Consent will be sought regarding matters of non-statutory use of personal data such as the use of images and names in publicity materials on induction or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

- 7.3 In relation to all students under the age of 12 years old we will seek consent from an individual with parental responsibility for that student.
- 7.4 We will generally seek consent directly from a student who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.
- 7.5 If consent is required for any other processing of personal data of any data subject, then the form of this consent must:
- a. inform the data subject of exactly what we intend to do with their personal data
 - b. require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
 - c. inform the data subject of how they can withdraw their consent.
 - d. Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.
- 7.6 The DPO must always be consulted in relation to any consent form before consent is obtained.
- 7.7 A record must always be kept of any consent, including how it was obtained and when.

Rights of the data subject

- 8.1 All people having personal data stored by the school have the right to:
- a) obtain from the School confirmation if personal data concerning him or her (or their child) is being processed;
 - b) Where this is the case, have a copy of the personal data and the following information:
 - (i) the purposes of the processing;
 - (ii) the third parties that the data will be shared with;
 - (iii) the period for which the personal data will be stored;
 - (iv) the existence of the right to request from the school to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held;
 - (v) the right to lodge a complaint with a supervisory authority;
 - (vi) where the personal data is not collected from the data subject, any available information as to its source.
 - c) if exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.
- 8.2 The school will place on its website a Privacy Notice¹ regarding the personal data held about students and why it is processed. Privacy Notices for workforce and

¹ <https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notice> or contact dposchools@somerset.gov.uk for adapted versions

- governors will be distributed to data subjects and be held on the school network.
- 8.3 Access to the data is called a **Subject Access Request**. Any person who wishes to exercise this right (or their parental right) should make a request (which does not need to be in writing) and submit it to the Headteacher.
- 8.4 The process for dealing with a Subject Access Request is outlined in **Appendix 5**.
- 8.5 The school aims to comply with requests for access to personal information as quickly as possible and in accordance with advice from the ICO and other professional agencies.
- 8.6 For further information on how the school upholds the rights of the data subject please see **Appendix 1.3**

Freedom of Information request policy

- 9.1 The Local Governing Body is committed to openness and transparency and this policy sets out the procedures and obligations on the school when a Freedom of Information request is received.
- 9.2 The Freedom of Information Act allows anyone to request information without giving a reason. The request must though state the name and address of the person as well as what information they are seeking. When a request is received this will be considered and the information, if held, will be provided unless one of the exemptions in the Act applies.
- 9.3 **Making requests:** Requests for information should be made clear and addressed to the school contact.
- 9.4 **Responding to requests:** Any request made to the school will be complied with in accordance with the time limits in the Act. For schools, this is 20 school days (i.e. not including weekends, holidays or school closure days) or 60 working days if this is shorter. The school will inform the DPO of the request.
- 9.5 **Charges:** The school will respond to most requests free of charge, and only charge where significant costs are incurred. The school may choose to charge a fee for complying with requests for information under FOI. The fees will be calculated according to FOI regulations and the person notified of the charge before information is supplied. The school reserves the right to refuse to supply information where the cost of doing so exceeds the statutory maximum. *Refer to the RHT FOI Publication Scheme*
- 9.6 **Exemptions:** Whenever a request for information is received it will be reviewed with consideration given to whether one of the exemptions set out in the Act applies. Common exemptions include the data protection of others, confidentiality, the request going beyond the costs limit and prejudice being caused to the effective conduct of public affairs. There are other exemptions that may also be relevant. Where an exemption is being relied on to prevent disclosure of information, we would inform you that this is the case in our refusal notice.
- 9.7 **Publication scheme:** This guide can be accessed at the following link

- 9.8 **Complaints:** Anyone who has made an FOI request to the school and who is not happy with the response that has been received can have an internal review of how their request has been handled. This will be generally carried out by a senior member of staff who was not involved in the initial request response. If a requester wishes to have an internal review, this should be requested within two months of the initial decision being communicated. Once an internal review request is received, we aim to conclude the review and communicate the outcome of this within 20 school days. Following an internal review, if the requester is still not happy with the response, they have the right to complaint to the Information Commissioner's Office.
- 9.9 The process and record keeping for FOI requests is given in **Appendix 6**.

Data security

- 10.1 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.
- 10.2 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.
- 10.3 Security procedures include:
- a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Headteacher.
 - b. **Staff network and software permissions.** Staff will only have the level of permissions required for their role. When staff leave the school all their permissions and accounts will be deleted.
 - c. **Data walks.** The DPL and governor conduct an annual data walk to assess the risk of data loss around the school, including physical security. The record of the walk and findings forms part of our monitoring documentation.
 - d. **Data on display.** All personal data on display has been assessed for risk and minimised where necessary. Consent has been sought for display where we do not have a legal, public interest, or legitimate interest in displaying the personal data.
 - e. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind, or information which would cause distress or harm if it was disclosed. Student exercise books are not locked away as we have assessed the risk of data loss to be disproportionate to the cost of storage.
 - f. **Privacy Impact Assessments.** In line with Data Protection legislation, the school will carry out a Privacy Impact Assessment when using software or online tools which may, if breached, cause harm to the rights and freedoms of individuals. These risk assessments will be carried out with the support of the DPO (see **Appendix 4 Privacy Impact Assessment**). The risk of data being transferred in and out of the UK will also be assessed.
 - g. **Methods of disposal.** Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required. IT

assets are disposed of in accordance with the ICO's guidance on the disposal of IT assets.

- h. **Data retention.** To minimise the risk of data being lost or mishandled, we will not retain data including emails any longer than is required by law or where there is a business need. **See paragraph 12 Data retention policy.**
- i. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended.
- j. **Working away from the school premises – paper documents.**
Staff are permitted to take children's work/exercise books and mark books home, ensuring that they are stored safely, e.g. when in transit, car doors to be locked if leaving vehicle. Staff are discouraged to take home documentation such as SEND reports, but on occasion this may be necessary. When necessary, such documentation should be stored securely in folders marked confidential and be stored in closed bags so cannot be seen. e.g. through a car window. All staff are responsible for the safe handling of pupil personal data when taken off-site and any loss or disclosure to third parties must be reported to the school data protection lead as soon as possible.
- k. **Working away from the school premises – electronic working.**
Staff are encouraged to access electronic documents via remote secure home access. When this is not possible, the school provide encrypted data sticks to store any data. If staff are using personal devices e.g. laptops and PCs for school business, care must be taken to ensure that family members or other third parties do not access any information relating to pupils at the school. A personal laptop or PC must have up to date virus protection. If staff believe pupil personal data may have been disclosed to third parties, this must be reported to the school data protection lead as soon as possible.
- l. **Document printing.** Documents containing personal data must be collected immediately from printers and not left on photocopiers.

10.4 Specific cybersecurity measures include:

- a. **In the event of a cyberattack.** Staff must follow the school's procedure e.g. turn off device and inform the school office and do not connect device to the school network until it has been checked by the Trust's IT staff . If systems are infected, the school will follow the Business Continuity Plan and inform the Trust's IT technician and Action Fraud. If personal data has been accessed, disclosed or is irretrievable, the school will follow the Data Breach procedure in Section 11.
- b. **Password security.** Staff are encouraged to change network passwords every 90 days and passwords must be complex and not repeated. Staff will be reminded to change their email passwords annually, particularly if they have never changed their password since their account has been created. Passwords will not be shared with any other user.
- c. **Admin password security.** The school will retain all high-level login details for their systems including administrator passwords for the network, wireless connections, anti-virus, remote learning systems. The login details will be kept securely in the school office.
- d. **Permissions.** User access to systems will be regularly reviewed by the school technician and access will be removed or downgraded when no longer required e.g. when a user has left the school. All access will be reviewed annually as part of end of year tasks.
- e. **Anti-virus and firewall protection.** The school will have appropriate systems in place to protect against cyberattack, ransomware and compromised accounts. This will be annually checked by the school technician.

- f. **Encryption.** All devices that have access to data attached to the network are fully encrypted in line with current guidance from the Trust's IT Team and/or Schools ICT at Somerset County Council.
- g. **Personal devices.** Personal devices may connect to the network with SLT permission but in full compliance with the ICT policies and this permission may be withdrawn at any time. The school's IT support will inform the owner/user that if a mobile device connects to the internet connection, then the device's online activity will be monitored and logged by the School's Internet Service Provider.
- h. **Back-ups.** Information including data in SIMS and the school network drives is backed up onsite/remotely as appropriate at regular intervals determined by the school's technical support. The Trust's IT Team will carry out annual testing of the back-ups to ensure that information can be restored in the event of the systems being compromised.
- i. **Staff cybersecurity training.** Staff will complete the [National Cyber Security Centre's online training module](#) to increase awareness of possible risk. This will be part of induction for new staff and a requirement for existing staff.
- j. **Acceptable User Policies.** Staff and learners will sign and follow the Trust's appropriate Acceptable Use Policies. The Trust's IT technical support will sign and follow the specific AUP for technicians.

10.5 Any member of staff found to be in breach of the security measures may be subject to disciplinary action.

Data breaches

- 11.1 If there is a data breach, the school/the Trust will inform the DPO who will then advise on any actions.
- 11.2 Any data breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken as shown in **Appendix 7**.
- 11.3 If there is judged to be a significant risk to the rights and freedoms of the affected data subject, the school/The Trust will communicate the breach to the data subjects with the support of the DPO.
- 11.4 In the case of a personal data breach where there is a significant risk of harm to the rights and freedoms of data subjects, the ICO should be informed as soon as possible and **within 72 hours of notification**. Further investigation of the breach can take place after this notification in line with advice from the DPO and the ICO.
- 11.5 Data breaches are reported using the information found at on the ICO website <https://ico.org.uk/for-organisations/report-a-breach/> and <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK-GDPR/personal-data-breaches/>
- 11.6 When reporting a breach, Data Protection legislation states that we must provide:
 - a. a description of the nature of the personal data breach including, where possible;
 - b. the categories and approximate number of individuals concerned; and
 - c. the categories and approximate number of personal data records concerned;
 - d. the name and contact details of the data protection officer or other contact point where more information can be obtained;

- e. a description of the likely consequences of the personal data breach; and
- f. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Data retention policy including emails

- 12.1 The Trust and its schools have responsibilities under the Data Protection Principles to keep data only for as long as necessary.
- 12.2 In respect of the length of time that the Trust and the schools should keep the data, they will follow the advice from the IRMS using their Records Management Toolkit for schools².
- 12.3 Emails containing personal information of students or staff members which may be required for learning or safeguarding purposes are attached to the student or staff members SIMS or CPOMS / My Concern / Safeguarding folder and permanently deleted from our email system.
- 12.4 If paper is due to be destroyed it will be cross-cut shredded either by the Trust or the school or by a commercial company.
- 12.5 If data is held on electronic devices then this will be deleted in line with the advice from the ICO³
- 12.6 A record should be kept of the data destroyed and/or the certificate of destruction issued by a third party.

Reporting policy incidents

- 13.1 Any member of the school staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Headteacher or for Trust staff, the Chief People Officer.

Monitoring and evaluation

- 14.1 This policy will be monitored and reviewed in line with the Trust's policy review procedure.

Links with other policies

- 15.1 This policy is linked to:
 - Freedom of Information Publication Scheme
 - E-Safety Policy
 - RHT Acceptable User Agreements

² <http://irms.org.uk/page/SchoolsToolkit>

³ <https://ico.org.uk/for-the-public/online/deleting-your-data/>

Appendix 1.1: Data Protection terms and definitions

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Asset Audit	The inventory of all the data processed by the school (or Trust) including the lawful basis for processing, who it is shared with, where it is transferred (including out of the UK) and how long it is retained for,
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes students, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living 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 such as a username or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

Appendix 1.2: Data Protection principles

Anyone processing personal data must comply with the data protection principles.

These provide that personal data must be:

- processed fairly and lawfully and transparently in relation to the data subject
- processed for specified, lawful purposes and in a way which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose
- processed securely using appropriate technical and organisational measures.

Personal data must also:

- be processed in line with data subjects' rights (see Appendix 1.3)
- not be transferred to people or organisations situated in other countries without adequate protection.

Appendix 1.3: Rights of the data subject and how we uphold them

1. **The right to be informed:** Data subjects are informed of how we process their personal data through Privacy Notices.
2. **The right of access:** Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the school's Subject Access Request Procedure.
3. **The right to rectification:** If a data subject informs the school or Trust that personal data held about them is inaccurate or incomplete, then we will consider that request and provide a response within one month. If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case. We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the ICO at the time that we inform them of our decision in relation to their request.
4. **The right to erasure:** Data subjects have a right to have personal data about them held by the school or Trust erased only in the following circumstances.
 - Where the personal data is no longer necessary for the purpose for which it was originally collected.
 - When a data subject withdraws consent – which will apply only where the school or Trust is relying on the individual's consent to the processing in the first place.
 - When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
 - Where the processing of the personal data is otherwise unlawful.
 - When it is necessary to erase the personal data to comply with a legal obligation.
 - If the school offers information society services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

The school or Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- to exercise the right of freedom of expression or information
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- for public health purposes in the public interest
- for archiving purposes in the public interest, research or statistical purposes
- in relation to a legal claim.

If the school or Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort. The DPO must be consulted in relation to requests under this right.

5. **The right to restrict processing:** Data subjects have a right to 'block' or suppress the processing of personal data. This means that the school or Trust can continue to hold the personal data but not do anything else with it.
The school / Trust must restrict the processing of personal data:
 - where it is in the process of considering a request for personal data to be rectified (see above)

- where the school or Trust is in the process of considering an objection to processing by a data subject
- where the processing is unlawful, but the data subject has asked the school or Trust not to delete the personal data
- where the school or Trust no longer needs the personal data but the data subject has asked the school or Trust not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the [Trust/Academy/School].
- If the school or Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort. The DPO must be consulted in relation to requests under this right.

6. **The right to data portability:** In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation. If such a request is made, then the DPO must be consulted.
7. **The right to object:** In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest. An objection to processing does not have to be complied with where the school or Trust can demonstrate compelling legitimate grounds which override the rights of the data subject. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right. In respect of direct marketing any objection to processing must be complied with. The school or Trust is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.
8. **Rights in relation to automated decision making and profiling:** Note: We will carefully consider whether it takes any decisions about any individuals by automated means. This includes any decisions made solely by automated means, and which has a legal effect in relation to the individual. This might include, for example, a decision as to whether to employ an individual. We consider it to be unlikely that this would apply to a Trust or school as there is always likely to be an element of human intervention in any decision making. However careful consideration should be given to this issue.

Appendix 2: Role of the Data Protection Officer

Purpose

The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee and verify the school's data protection processes and advise the school on best practice.

Within each school there will be a Data Protection Lead (DPL), who maintains contact with the DPO and is responsible for assisting in monitoring with compliance and verifies the school's data protection practices on a day to day basis.

Data Protection Officer Responsibilities

To:

- advise the school about their obligations under the UK General Data Protection Regulation and the Data Protection Act 2018;
- support the DPL in developing a joint understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPL, with the monitoring of the school's compliance with data protection law, by:
 - collecting information to identify data processing activities;
 - analysing and checking the compliance of data processing activities;
 - informing, advising and issuing recommendations to the school;
 - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPL in making sure that the school's policies are followed, through:
 - assigning responsibilities to individuals;
 - awareness-raising activities;
 - coordinating staff training;
 - conducting internal data protection audits;
- advise on and assist the school with carrying out data protection privacy impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
 - helping the ICO to access documents and information;
 - seeking advice on data protection issues;
- act as a contact point for individuals whose data is processed (for example, staff, students and parents), including:
 - responding with support from the DPL to subject access requests;
 - responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:

- prioritising the higher-risk areas of data protection and focusing mostly on these
- advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO/DPL roles should involve.
- report to the governing board/board of trustees on the school's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- assist the DPL in maintaining a record of the school's data processing activities;
- work with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPL in fostering a culture of data protection throughout the school;
- work closely with other departments and services to ensure UK GDPR compliance, such as HR, legal, IT and security;
- work with the Senior Leadership team at the school to ensure UK GDPR compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for the school;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;
- providing materials and advice in completing a dynamic Data Asset Audit and assisting in its completion if necessary;
- checking issues with the Data Asset Audit;
- providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues;
- acting as the point of contact for SAR and FOI requests and supporting the school to provide the information as required;
- providing a Data Protection Audit on a 3-yearly rota basis and producing a report for Governors at cost;
- providing telephone and email advice and support;
- providing regional training for the DPL and other staff;
- providing school based on-demand training at cost.

Appendix 3: Role of the Data Protection Lead

Data Protection Lead Responsibilities

To:

- verify that the school has registered with the ICO;
- support the DPO in advising the school about their obligations under the Data Protection Act 2018;
- support the DPO in developing an understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPO, with the monitoring of the school's compliance with data protection law, by:
 - collecting information to identify data processing activities;
 - analysing and checking the compliance of data processing activities;
 - informing, advising and issuing recommendations to the school;
 - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPO in making sure that the school's policies are followed, through:
 - assigning responsibilities to individuals;
 - awareness-raising activities;
 - coordinating staff training;
 - conducting internal data protection audits;
- act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, students and parents), including:
 - responding with support from the DPO to subject access requests;
 - responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used;
- assist the DPO in maintaining a record of the school's data processing activities providing this on a yearly basis to the DPO;
- assisting the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPO in fostering a culture of data protection throughout the school;
- work with the Senior Leadership team at the school to ensure UK GDPR compliance;
- assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the point of contact with the DPO;
- assist in customising the Data Protection Policy for the school;

- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- providing materials and advice in completing a Data Asset Audit and assisting in its completion if necessary;
- supplying the DPO with the Data Asset Audit on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Appendix 4: Privacy Impact Assessment

Before the use of any new service that uses personal data, staff should fill in a **Privacy Impact Assessment Form**.

The Senior Leaders and/or the DPL, with advice from the DPO will then approve the use and the information be placed on the Data Asset Audit.

Privacy Impact Assessment Form

Privacy Impact Assessment (PIA) for:

Name of Service/Software/App

Data Protection Principles

- processing to be lawful and fair
- purposes of processing be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions

We need to complete this form because:

- the use involves the collection of new information about individuals;
- the use compels individuals to provide information about themselves;
- the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- we are using information about individuals for a purpose it is not currently used for, or in a way it is not currently used
- we are using new technology that might be perceived as being privacy intrusive, for example, the use of biometrics or facial recognition;
- the use results in us making decisions or acting against individuals in ways that can have a significant impact on them;
- the information about individuals is of a kind particularly likely to raise privacy concerns or expectations, for example, health records, criminal records or other information that people would consider to be private;
- the use requires us to contact individuals in ways that they may find intrusive.

Privacy Impact Assessment Form

Describe the service

Describe the data collected and the possible uses of the data

List of data held

Collection of data

Possible uses

Identify the privacy, related risks and possible solutions
To be discussed with the Data Protection Lead

Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
1.	•	•	•
2.	•	•	•
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•

Sign off and notes

Comments on risks

Processes that must be in place

Contact point for future privacy concerns

Data Protection Officer:

dposchools@somerset.gov.uk

Data Protection Lead:

Date completed:

Appendix 5: Subject Access Request process

On receiving a Subject Access Request or request for change or deletion of data the DPO or school will:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- contact the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **30 calendar days**, which can be extended by a further 2 months where the request is complex or where there are numerous requests. *Note Time for processing a request for an educational record in a maintained school is 15 days.*

Schools can refuse a request if the request is unfounded or excessive; this might be where the request is repetitive, malicious or asks for further copies of information previously supplied.

Schools can also refuse a request to disclose information if:

- sharing the data would cause serious harm to the physical or mental health of an individual.
- a child is at serious risk of abuse and where disclosure would not be in the child's best interests.
- It is contained in adoption or parental order records.
- It is given to a court in proceedings concerning the child.
- The information includes other people's personal data unless the other individual has consented to the disclosure. Note: it is reasonable to disclose information about 'education-related' workers as long as the information relates to their employment e.g. a request for a pupil report written by a teacher.

If you're unsure about whether you can refuse a request, contact the ICO for advice.

The Subject Access Requests are held here: Securely in the School Office

Subject Access Request Record

Name of data subject: _____

Name of person who made request: _____

Date request received: _____ / _____ / _____

Contact DPO (dposchools@somerset.gov.uk) : _____ / _____ / _____

Date acknowledgement sent: _____ / _____ / _____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: _____ / _____ / _____
(within 30 days of request)

Signed off by: _____

Appendix 6: Freedom of Information request process

On receiving a Freedom of Information Request, which must be made in writing, the DPO or the school will:

- inform the DPL in the school (and the Headteacher if necessary);
- contact the DPO for clarity on the request and procedure, and a sample response
- record the details of the request, updating this record where necessary (see next page);
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- decide that if the material is already published or falls within an exemption;
- if data is not going to be published inform the requestor why this is not being released;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **20 school days** (i.e. not including weekends, holidays or school closure days) or **60 working days** if this is shorter.

The Freedom of Information requests are held here: Securely in the School Office

Freedom of Information Request Record

Name of person who made request: _____

Date request received: _____ / _____ / _____

Contact DPO (dposchools@somerset.gov.uk) : _____ / _____ / _____

Date acknowledgement sent: _____ / _____ / _____

Name of person dealing with request: _____

	Notes (Overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, then refer them to the correct agency
Do you need to exempt/redact data?	Could the data identify individuals Are any of the answers less than 5 people – use '5 or less including zero)? Are their commercial sensibilities?
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

At all stages, your DPO or DPL will be able to provide you with advice.

Date request completed: _____ / _____ / _____
(within 20 days of request)

Signed off by: _____

Appendix 7: Data Breach process

Every Data Protection Breach should be recorded. The process that should be followed is listed below:

- inform the DPL in the school (and the Headteacher if necessary);
- record the details of the breach providing these details:
 - a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and
 - the categories and approximate number of personal data records concerned;
 - the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
 - a description of the likely consequences of the personal data breach; and
 - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
- contact the DPO if clarity on reporting the breach is needed and if necessary, report to the ICO;
 - either by phoning 0303123 1113
 - By filling in the form at:
<https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc>
and sending it to casework@ico.org.uk
- updating this record where necessary (see next page);
- identify the people whose data is accidentally released, inform them of the breach and the processes taken to rectify the situation;
- review why the breach took place and if future similar events can be avoided.

The Data Protection Breach records requests are held here: Securely in the School Office

Data Breach Record

Date: / /	Person responsible for dealing with breach				
Description of the nature of the personal data breach – how it occurred					
The categories and approximate number of individuals concerned					
The categories and approximate number of personal data records concerned					
A description of the likely consequences of the personal data breach					
A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects					
Reported by					
Phone/email sent to DPO dposchools@somerset.gov.uk	y/n	Is this high risk?	y/n	Report to ICO	y/n
Date reported to data subjects					
Notes					
Actions approved by		Date	/ /		