

# Terms of Reference for the **INFORMATION SECURITY LEAD GOVERNOR** (inc. General Data Protection Regulation (GDPR)) at Bow Community Primary School

Agreed at the meeting of the full governing board on: [21 September 2021](#)

Review date: [September 2022](#)

Name of the GDPR Governor: Tony Neal

**Policies and Documents delegated to this governor:**

- Data Protection Policy (Statutory)
- Freedom of Information Procedure
- Information Security Policy
- Information Security Incident Management Policy
- Information Security Incident Management Procedure
- Privacy Notice for Volunteers
- Retention and Disposal Policy
- GDPR Data Subject Request Procedure
- Video Conferencing Policy

**Duties which are delegated to this governor:**

*It is the overall Governing Board, however, that in all cases remains accountable in law and to Ofsted for the exercise of its functions.*

**D** Delegated to Lead Governor; report to FGB      **R** Recommend to Full Governing Board

The GDPR governor will undertake appropriate governor training in order to fully understand their role including, where possible and appropriate, joining relevant staff training to keep updated.	<b>D</b>
Understand the role of the Data Protection Officer (DPO), and be clear that, as a public authority, each school must designate a named DPO in order to be comply with new legislation.	<b>D</b>
Ensure that the school has appointed an appropriate Data Protection Officer (DPO) or subscribes to a reputable DPO service.	<b>D</b>
To ensure the statutory duties relating to pupil record keeping, disclosure of information and pupil reports are fulfilled. Including reviewing and updating the Data Protection Policy, the Freedom of Information Publication Scheme and Privacy Notices in consultation with the DPO. Monitor that the DPO has provided appropriate annual training for staff, governors and the school can demonstrate compliance with Data Protection Law.	<b>D</b>
Seek confirmation from the DPO that the school is registered with the Information Commissioners Office (ICO) as a Data Controller.	<b>D</b>
Working with the DPO, ensure that governors are aware that responsibility for compliance with data protection legislation lies with them and that they are kept informed about all key issues arising for the schools from legislative changes and understand how to effectively monitor and review compliance.	<b>D</b>
Liaise with the DPO to monitor and evaluate any data breaches and near misses to identify any changes in practice or training required. Ensure that any notifiable breaches are reported to the board.	<b>R</b>
Ensure that Privacy Notices are in place for governors explaining how information will be used,	<b>R</b>

shared and published.	
Engage in discussions about identification and mitigation of risks.	D
Check that the school has good network security to keep the personal data they hold protected including phishing awareness. This should also include having a school emergency plan in place that has cyber resilience as a consideration.	D
Seek assurance from the DPO that the school can demonstrate compliance with Data Protection Regulations.	D
Ensure the school has a process in place for dealing with a Subject Access Request (SAR). Monitor the number of requests received and assess if there are any recurring themes which may identify areas for improvement in the way the school is handling data.	D
Review of data protection policies in light of any changes to procedures and processes arising from the data audit and risk management.	D
Seek assurance from the DPO that the school has a Retention Schedule in place for data, including data relating to governors at the school.	R
Check that the school has an ICT Acceptable Use policy in place for staff and that all staff have been made aware of their responsibilities and have signed to accept them.	D
Verify that the school has a process in place to seek and record consent where required from staff, parents and governors.	D
To ensure the statutory duties relating to pupil record keeping, disclosure of information and pupil reports are fulfilled. Including reviewing and updating the Data Protection Policy and the Freedom of Information Publication Scheme, in consultation with the DPO. Monitor that the DPO has provided appropriate training for staff, governors and the school can demonstrate compliance with Data Protection Law.	D
Seek confirmation from the DPO that the school is registered with the Information Commissioners Office (ICO) as a Data Controller.	D
Working with the DPO, ensure that governors are aware that responsibility for compliance with data protection legislation lies with them and that they are kept informed about all key issues arising for the schools from the legislative changes and understand how to effectively monitor and review compliance.	D
Liaise with the Data Protection Officer (DPO) to monitor and evaluate any data breaches and near misses to identify any changes in practice required. Ensure that any notifiable breaches are reported to the board.	D
<b>Online Safety</b>	
To monitor and evaluate the online safety policy and report to FGB. Policy/guidance on the use of mobile technology for both staff and pupils needs to be present (this could be part of online safety policy or acceptable user policy; models are available from the Governance Consultancy team).	D
To monitor and evaluate the school's effective application of the online safety policy.	D
To ensure that the school follows all current online safety advice and keeps the children and staff safe.	D
To support the school in encouraging parents and the wider community to become engaged in online safety activities.	D

The GDPR lead and other members of the board may wish to refer to the GDPR Q-card on the Governance Consultancy team website

<https://www.babcockldp.co.uk/improving-schools-settings/governance-consultancy/q-cards>

and the DfE Data Protection Toolkit for schools

<https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>

