Hedingham School and Sixth Form

Information Governance Framework Policy

Supporting effective corporate management of Information Governance activities

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: All employees must **comply** with all Information Policies
2. ***MUST***: All employees must successfully complete relevant **training** in Information Governance key messages annually
3. ***MUST***: All **managers** must ensure that employees under their management are complying with our policies and any agreed exceptions
4. ***MUST***: We must ensure that the **roles** of Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO) are in place
5. ***MUST***: We must ensure that an Information Governance Strategy is in place
6. ***MUST***: We must undertake annual **reviews** of the IG Strategy, all Information Policies and Information Risks
7. ***MUST***: Any **exceptions** to Information Policies must be risk assessed and approved

Why must I do it?

1. This is to ensure that the Organisation remains complaint with Information law and provides assurance to the public over secure practices.
2. This is to ensure that ECC can be certain that staff have been told the correct messages about how to handle data securely, and that we can evidence this to our regulators, partners and the public to give them confidence that we are suitable custodians of their data
3. Managers have a key role in ensuring any policy is being implemented appropriately.
4. The DPO role is a statutory requirement and the SIRO is best practice.
5. Strategies are only effective when they meet the demands of the law and enable employees to achieve compliance in a practical way. It is therefore vital that our strategy reflects the current legal requirements and helps guide employees in a clear way to meet those requirements. The Strategy must therefore be regularly reviewed to ensure it is fit for purpose.
6. Policies are only effective when they meet the demands of the law and enable employees to achieve compliance in a practical way. It is therefore vital that our policies reflect the current legal requirements and help guide employees in a clear way to meet those requirements. Policy and Risk Management must therefore be regularly reviewed to ensure they are fit for purpose.

7. We need to monitor and control the risks created by allowing exceptions to policy

How must I do it?

1. By reading the Information Policies, by attending and completing relevant training, by seeking clarification of policy from managers when unsure.
2. By attending face-to-face training or completing elearning that has been designated as mandatory for your role.
3. Ensure employees are instructed appropriately (through both Induction and Refresher training) on how to securely manage the data they have access to in their roles. Ensure employees have completed relevant formal training (for systems they use, and compulsory E-Learning). Use team meetings to discuss information policy issues. Where there is uncertainty over correct procedure, seek advice for clarification.
4. Appoint new employees or add responsibilities to existing roles. Ensure that the responsibilities of the roles are fully documented and that the role holders have sufficient resource and training to fulfil their roles.
5. A Strategy should be approved by the Leadership Team and annual reviews should be made against its progress, reported to the Leadership Team and the Strategy should be amended if required.
6. Policy and Risk reviews should be undertaken annually and approved by the Leadership Team.
7. By recording approved exceptions in such a way as to be able to report on all current instances; showing who and what the exception is for, why it was granted, when the exception approval period comes to an end and who supported and approved the exception. Assessment of a request for an exception must be done by receiving an approval and acceptance of risk by the Senior Information Risk Owner (SIRO) or a delegated role.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Headteacher 01787 460470 - DataCompliance@hedingham.essex.sch.uk

Document Control

Version:	1
Date approved:	21.3.2018
Approved by:	Governing Body
Next review:	Spring 2019

References

- Data Protection Act 1998 (to May 25th 2018)
- General Data Protection Regulations 2016 (from 25th May 2018)
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.