



Information Governance Policy

Introduction

Information is a vital asset, both in terms of the information that we process and use for our clients and the efficient management of our services and resources. It plays a key part in supporting our clients and our service provision and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

Purpose of the policy

This Information Governance policy provides an overview of the organisation's approach to information governance (IG); a guide to the procedures in use; and details about the IG management structures within the organisation.

The organisation's approach to Information Governance

Turn IT on undertakes to implement information governance effectively and will ensure the following:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information governance training will be available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.



Procedures in use in the organisation

This Information Governance policy is underpinned by the following procedures:

- Records management procedure that set outs how client records will be created, used, stored and disposed of;
- Access control procedure that sets out procedures for the management of access to computer-based information systems;
- Information security procedure that sets out procedures around the transfer of confidential information;
- Incident management procedure that sets out the procedures for managing and reporting information incidents;
- Business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer systems;

Staff guidance in use in the organisation

Staff compliance with the procedures is supported by the following guidance material:

- Records management procedure: guidelines on good record keeping;
- Protecting Schools Data policy: sets out the required standards to maintain the confidentiality of schools' information; obligations around the disclosure of information and appropriately obtaining consent;
- Safeguarding consent form; ensures that staff have agreed to share the necessary data to allow schools' to conform to OFSTED requirements;
- Employee Data Policy; to ensure that staff understand what we hold and use their data for
- Data Protection Consent Form; to ensure that staff have signed to confirm that they have read and understood how we use their data
- Access control procedure: guidelines on the appropriate use of computer systems;
- Mobile Devices Policy: guidelines on maintaining confidentiality and security when working with portable or removable computer equipment;
- Information incidents guidelines: guidelines on identifying and reporting incidents.



Responsibilities and accountabilities

The designated Information Governance lead for the organisation is Head of HR & Finance (internal information) and Head of Data Protection (client information).

The key responsibilities of the leads are:

- Developing and implementing IG procedures and processes for the organisation;
- Raising awareness and providing advice and guidelines about IG to all staff;
- Ensuring that any training made available is taken up;
- Coordinating the activities of other staff given DP, confidentiality, information quality, records management and Freedom of Information responsibilities;
- Working with the IT team to ensure that data is kept secure
- Monitoring information handling in the organisation to ensure compliance with law, guidance and local procedures;
- Ensuring schools are appropriately informed about the organisation's information handling activities:
- Maintaining an Information Asset Register

The day to day responsibilities for providing guidance to staff will be undertaken by the HR and GDPR teams.

The owner of the organisation is Tom Welch and he is responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law and professional codes of conduct.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.