IPC SERVICES

Experience and Reliability

Records Management Policy

Last updated: 1 May 2018

Statement of intent

IPC Services is committed to maintaining the confidentiality of its information and ensuring that all records are only accessible by the appropriate individuals. In line with the requirements of the GDPR, the company also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

This policy has been created to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet statutory requirements.

This document complies with the requirements set out in the GDPR, which is effective of 25 May 2018.

It should be understood that there is not a sector wide data retention policy that prescribes how long data should be retained for. The retention periods outlined in this policy are good practice guidelines only.

The table for retention periods are based on information provided by the Information Records Management Society (IRMS) and the DfE and are not an exhaustive list of records that may be kept.

Signed by:

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

1.2. This policy also has due regard to the following guidance:

- Information Records Management Society (2016) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data protection: a toolkit for schools'

2. Responsibilities

2.1. IPC Services has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The Data Protection Officer (DPO) holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The DPO is responsible for the management of records at IPC Services.

2.4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis.

2.5. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.

2.6. All staff members are responsible for ensuring that any records for which they are responsible are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy

3. Retention of records

3.1. The table below outlines the retention periods for records, and the action that will be taken after the retention period, in line with any requirements.

3.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Agenda for governing board meetings	For one academic year	Securely disposed of
Original, signed copies of the minutes of governing board meetings	Permanent	These will be retained electronically for the duration of the contract; these will be securely transferred if the contract ceases.
Reports presented to the governing board	For one term (schools and academies are expected to retain these for one academic year)	Securely disposed of
Instruments of government, including articles of association	Permanent	These will be retained for the duration of the contract.

4. Storing and protecting information

4.1. The DPO will undertake a risk analysis to identify which records require retention; these records will be stored in the most secure manner.

4.2. The DPO will ensure regular back-ups of information to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

4.3. Confidential paper records are kept in a secure area with restricted access.

4.4. Confidential paper records are not left unattended or in clear view when held in a location with general access.

4.5. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

4.6. Where data is saved on removable storage or a portable device, the device is kept in a lockable cabinet with restricted access.

4.7. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

4.8. All electronic devices are password-protected to protect the information on the device in case of theft.

4.9. All members of staff are provided with their own secure login and password; staff receive regular prompts to change their password.

4.10. Circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

4.11. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

4.12. Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

4.13. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a secure area with restricted access.

4.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times.

4.15. IPC Services takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

4.16. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

4.17. Any damage to or theft of data will be managed in accordance with the data protection policy.

5. Disposal of data

5.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

5.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut.

5.3. Where information has been kept for administrative purposes, the DPO will review the information again each year. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every year

5.4. Where information must be kept permanently, this information is exempt from the normal review procedures.

6. Monitoring and review

6.1. This policy will be reviewed on an annual basis by the DPO – the next scheduled review date for this policy is April 2019.

6.2. Any changes made to this policy will be communicated to all members of staff.