Thoughts of Others Limited
Data Protection Legislation Framework (GDPR)

Version	Purpose / Change	Author	Date
1	Document created, in line with current legislation	Chris Delahaye	May 2018

Policy Statement

On the 25th May 2018 the General Data Protection Regulations (GDPR) replaces the Data Protection Act 1998 in its entirety and will form the basis of the Data Protection Act 2018, entrenching its principles in domestic law. It replaces the existing Data Protection Laws to make them fit for the digital age in which personal data is increasingly being processed. The Act sets new standards for protecting personal and sensitive data. It gives people more control over the use of their data and assists in the preparation for a future outside of the EU.

There are 4 main matters provided for, these are:

- General Data Processing
- Law Enforcement Data processing
- Data Processing for National Security Purposes
- Enforcement

All of the above need to be set in the context of international, national and local data processing systems which are increasingly dependent upon internet usage for exchange and transit of data. The UK must lock into international data protection arrangements, systems and processes and this Act updates and reinforces the mechanism to enable this to take place.

Given the size of the legislation and some of the media hype surrounding its introduction this policy is written in two Sections.

Section 1 Overview of the Act
Section 2 The Policy

Section 1

Overview of the Act

The Act is structured in 7 parts, each of which covers specific areas. These are:

Part 1: Preliminary

This sets out the parameters of the Act, gives an overview, explains that most processing of personal data is subject to the Act and gives the terms relating to the processing of personal data.

Part 2: General Processing

This supplements the GDPR and sets out a broadly equivalent regime to certain types of processing to which the GDPR **does not** apply.

Part 3: Law Enforcement Processing

This covers:

- "competent authority"
- meaning of "controller" and "processor"
- data protection principles
- safeguards in regard to archiving and sensitive processing
- rights and access of the data subject, including erasure
- implements the law enforcement directive
- controller and processor duties and obligations
- records
- cooperation with the ICO commissioner
- personal data breaches
- the remedy of such breaches
- position of the data protection officer and their tasks
- transfer of data internationally to particular recipients
- national security considerations
- special processing restrictions and reporting of infringements.

Part 4: Intelligence Services Processing

This covers only data handled by the above e.g. MI5 and MI6 and includes rights of access, automated decisions, rectification and erasure, obligations relating to security and data breaches.

Part 5: The Information Commissioner

This covers:

- general functions including publication of Codes of Practice and guidance
- their International role
- their responsibilities in relation to specific Codes of Practice
- consensual audits
- information to be provided to the Commissioner
- confidentiality and privileged communication
- fees for services
- charges payable to the commission
- publications
- Notices from the Commissioner
- reporting to parliament.

Part 6: Enforcement

This covers the new enforcement regime in relation to all forms of Notice issued by the Commissioner:

- powers of entry and inspection
- penalty amounts
- appeals
- complaints
- remedies in the court
- offences
- special purpose proceedings.

Part 7: Supplementary and Final Provision

This covers legal changes which the new Act alters in relation to other legal matters, e.g. Tribunal Procedure rules, definitions, changes to the Data Protection Convention etc. and List of Schedule(s).

Statement of Intent

As you can see, this Act is a huge piece of legislation, the majority of which is outside the remit of service providers working within the Adult Health and Social Care Sector. The I.C.O. confirms that many concepts and principles are much the same and businesses already complying with the current law are likely to be already meeting many of the key requirements of the GDPR and the new Act.

The Information Commissioner says the new Act represents a “step change” from previous laws. “It means a change of culture of the organisation. That is not an easy thing to do, and it's certainly true that accountability cannot be bolted on: it needs to be a part of the organisation’s overall systems approach to how it manages and processes personal data”. It’s a change of mindset in regard to data handling, collection and retention.

We need to stop taking personal data for granted, it's not a commodity we own: it's only ever on loan. Individuals have been given control and we have been given fiduciary duty of care over it.

As an organisation handling personal data on a day to day basis, this policy sets out the requirements of the new Act and how we, as an organisation will meet our legal obligations. Staff awareness and understanding of their responsibilities in regard to the handling, collection and retention of data will be core to the successful embedding of this policy.

Preparation: (The 12 Steps)

In order to comply with the requirements of the Act preparation will include the completion of *Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now:* https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

- Awareness
- Information we hold
- Communicating privacy information
- Individuals rights
- Subject access requests
- Lawful bases for processing
- Consent
- Children
- Data Breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officers
- International Data

The ICO has issued this guidance as the start of the preparation. They have also made clear that they are aware that for small companies in particular time can be a factor in this preparation, but it is important to remember that you must start the 12 steps in order that you can show compliance. As an organisation we are preparing for this new Act by completing these 12 steps.

Privacy notices, transparency and control

To start off a privacy notice, you need to tell people, as a minimum

- who you are
- what you are going to do with their information
- who it will be shared with.

Being transparent, and providing accessible information, is core to compliance and the GDPR. Privacy notices is the most common way to meet the GDPR requirements.

Transparency, in a governance or business context, is honesty and openness and the more transparent we can be the more easily understood and accessible our services become to the people who use them.

In the context of data processing is simply that:
"it should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of their personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processor and further information to ensure fair and transparent processing in respect of the confirmation and communication of personal data concerning them which is being processed."

Information Commissioner: Role and Function

With regard to the changes within the new GDPR, National Supervising Authorities in all EU member states have had their powers of enforcement enhanced. The Information Commissioner's Office is the UK's supervising authority.

Within the Enforcement Toolbox, the I.C.O. can now issue substantial fines of up to 20 million, or, 4% of an organisation's global turnover for certain data protection infringements. Fines, when appropriate, will be of the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches.

The GDPR also empowers the I.C.O. to create tailor made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium sized organisations can take comfort in the

fact that they are unlikely to face the sort of punitive fines that rogue tech giants could in order to bring them to head.

The role and scope of the I.C.O. has not fundamentally changed, but rather has been expanded and enhanced via the new GDPR.

Codes of Conduct and Certification Mechanisms

Although the use of any of the above is encouraged by the GDPR, it is not obligatory. If an approved code of conduct or certification scheme becomes available that covers our processing activity, consideration will be given to working towards such a scheme as a way of demonstrating our compliance. The I.C.O. will develop its own code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct.

Derogations and Exceptions

The Act provides that member states of the EU can provide their own national rules in respect of specific processing activities.

All Data Controllers must be familiar with Schedules 1-18 of the GDPR as these are the lawful exemptions pertinent to many other legal frameworks and Acts. These Schedules cover things such as Parliamentary Privilege, Health and Social Work, Criminal Convictions (Additional Safeguards), Research, Statistics and Archiving, Education Child Abuse, and include specific provisions for data processing within the Schedule(s).

For example: Schedule 15: Powers of Entry and Inspection. This Schedule sets out clearly the powers of the Information Commissioner's Office in relation to warrant(s) issued by the courts which allow the I.C.O. to enter premises and inspect data field there, including the seizure of documents. Schedule 18 is where all the legislative changes, in all pertinent primary legislation is found, including the repeal of the Data Protection Act 1998. As the Act is embedded in to the organisation, Data controllers, their role and responsibilities, will need to be reviewed and revised to ensure compliance.

Codes of Practice

The Act enhances the role of the Information Commissioner's Office (I.C.O.) in the compilation of such Codes and these will be available in due course. It is important that we are regularly checking the I.C.O. website in order to keep up with current guidance.

Section 2

1. Rationale

This organisation aims to ensure that all data required for the delivery of the service and the lawful running of the organisation is collected, handled, maintained and stored in accordance to the requirements of the Data Protection Act 2018.

The General Data Protection Regulations (GDPR) form the basis of the Act but in order to be effective and compliant with its requirements, the Related Policy list below should be viewed as core to this policy, as should Section 1 and the Related Guidance links. The CCTV policy also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

PLEASE NOTE All Guidance from the ICO should be considered "Live Documentation" and regularly checked until all Codes of Practice and Guidance are issued. Working Party 29 known as WP29 is a representative body from each of the EU member states who have developed and worked on the Act. WP29 still sits and meets in the European Parliament until all of the complexities of the Act have been clarified and amended into law.

The organisation collects, processes and retains personal and sensitive data, as defined below, and holds responsibility as the Data Controller for the handling of such data in line with the relevant legislation, subject to third party data sharing agreements in which the data processor retains liability for breaches arising out of its processing activities. The organisation processes personal and sensitive information to enable the provision of quality care and education, the safeguarding of young people and others and associated functions. This policy applies to the personal and sensitive data of care users, pupils of Spring Hill High School, parents and carers, existing and former employees, volunteers and job applicants, current and previous residential and educational placements and other third parties who come into contact with the organisation ('relevant individuals').

The purposes of this policy are to enable to organisation to:

- Comply with our legal, regulatory and corporate governance obligations and good practice
- Gather information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensure the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigate complaints and respond appropriately to the requests of relevant individuals

- Check references, ensure safe working practices, monitor and manage staff access systems and facilities and absences, administration and assessments
- Monitor pupil progress, behaviour tracking and staff conduct/disciplinary matters
- Improve services

2. Definitions

The GDPR applies to “Controllers”, “Processors” and “Data Protection Officer” and to certain types of information, specifically, “Personal Data” and “Sensitive Personal Data” referred to in the Act as Special Categories of Personal Data”. The definition, role and duties of the Data Protection Officer are dealt with separately to this section.

“Controllers”

This role determines, on behalf of the organisation, the purposes and means of processing personal data.

“Processors”

This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations on you, e.g. you are required to keep and maintain records of personal data and processing activities. This role has legal liabilities if they are responsible for any breach.

“Personal Data”

This means information that relates to an identified or identifiable individual. So, if it is possible to identify an individual directly from the information you are processing, then that information may be personal data. this would include name, reference or identification number (for example UPN number), location data or online identifier. This reflects changes in technology which incorporates a wide range of different identifiers. Personal Data applies to both automated and physical filing systems. It can also apply to pseudonymised (e.g. key-coded) data, dependent on how difficult it is to attribute the pseudonym to a particular individual.

“Special Categories of personal Data”

This category of data is more sensitive and requires greater protection. Sensitive personal data specifically includes any data relating to an individual’s physical or mental health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership,

sex life or sexual orientation. It also includes genetic and biometric data (related to the genetic characteristics of a person or data created for ID purposes such as facial scans etc). Safeguards apply to other type of data e.g. criminal convictions and offences; intelligence data etc. The organisation shall not process data relating to criminal convictions and offences unless authorised by Union or UK legislation or under the control of official authority.

"data breach"

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. Roles and Responsibilities

Board of Directors

The board has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The organisation shall ensure that the designated Data Protection Officer (DPO) is involved in all issues relating to the protection of personal information and shall support the DPO in performing the tasks below by providing the necessary resources and access to personal information and processing operations. The DPO shall be given no instructions in how to perform their duties, and shall not be dismissed or otherwise penalised for performing them. The DPO shall act impartially and have respect for confidentiality concerning the performance of the tasks below and shall avoid a conflict of interests in the performance of their duties.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Chris Delahaye
Data Protection Officer

cdelahaye@springhillhighschool.co.uk
0121 448 3001

Senior Leadership

The Home Managers, Head and Deputy Head Teachers acts as the representatives of the data controller on a day-to-day basis.

All Staff

Staff are responsible for:

- Collecting, storing and processing any personal or sensitive data in accordance with this policy
- Informing the organisation of any changes to their personal data, such as change of address
- Contacting the DPO in the following circumstances:

- with any questions about the operation of this policy, data protection law, retaining personal information or keeping personal information secure
- if they have any concerns that this policy is not being followed
- if they are unsure whether they have a lawful basis to use personal data in a particular way
- if there has been a data breach
- whenever they are involved in a new activity that may affect the privacy rights of relevant individuals
- if they have any questions regarding sharing personal data with third parties

Data protection and protecting the privacy rights of relevant individuals is the responsibility of all staff within the organisation. Significant breaches of this policy will be handled under Thoughts of Others Ltd's disciplinary procedures which may amount to gross misconduct.

4. Data Protection Principles

Please refer to the Related Guidance links for further information.
The GDPR sets out the following principles for which this organisation is responsible and must meet. The controller shall be responsible for, and be able to demonstrate, compliance with the principles below: (Article 5 (2) GDPR).

a) Processed lawfully, fairly and in a transparent manner (*Lawful basis for processing- see section 6*);

b) Be collected for specified, explicit and legitimate purposes. Further processing for archiving purposes in the public interest shall not be considered to be incompatible with the initial purpose (*purpose limitation*);

c) Adequate, relevant and limited to what is necessary to fulfil the specified purpose (*data minimisation*);

d) Accurate and up to date (*accuracy*);
Every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which allows identification of individuals for no longer than is necessary for the specified purpose (*storage limitation*);
Personal data may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (*see section 7.3*).

f) Processed in a manner that ensures appropriate security of the personal data (*integrity and confidentiality- see section 7.3*);
This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

5. Data Protection by Design and Default (*Appropriate Technical or Organisational Measures*)

The organisation's approach to information security is outlined in the *Information Security Policy*. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing *data protection impact assessments* where our processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Conducting bi-annual audits to test our privacy measures and make sure we are compliant

- Maintaining a *Record of Processing Activities*, which is an internal record of the type of data, relevant individual, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

6. Lawful basis for processing

The organisation shall carry out its processing activities under one of the following lawful basis:

- Consent: In some circumstances, we will require the relevant individual to give clear consent for us to process their personal data for a specific purpose. For example photographs and videos for promotion (see section 13 below)
- Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- Legal Obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
- Vital Interests: the processing is necessary to protect someone's life.
- Public Task: the processing is necessary for us to perform a task in the public interest, or for official functions with a clear basis in law.
- Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the relevant individual's personal data which overrides those legitimate interests. (This does not apply if a public authority is processing data to perform its official tasks).

For special categories of personal data as defined above, we will also meet one of the special category conditions for processing which are set out in the GDPR article 9 and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental or carer's consent where the pupil is under 13 (except for online counselling and preventive services).

Appendix 2 contains further guidance on the requirements of lawful bases.

7. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the organisation's *Information Security* policy.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

We need to liaise with other agencies such as health authorities in order to safeguard relevant individuals

Our suppliers or contractors need data to enable us to provide services to our staff, care users and learners – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

We have no intention to transfer data internationally across Union states or outside the European Economic Area (EEA).

9. Rights of Individuals

In addition to the right to be informed when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, providing there are no other legitimate reasons for continued processing
- Access the information held about you and the uses for which it was collected, providing there are not legitimate or lawful reasons to deny access
- Ask us to rectify inaccurate information or erase it, providing there are not legitimate or lawful reasons to retain it
- Restrict processing of their personal data, for a period to allow us to verify the accuracy of data or demonstrate our legitimate grounds for processing
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

All relevant guidance to individual rights is not yet complete, Working Party (WP)29 will continue to work and produce such guidance as is thought appropriate.

Any individual request which falls into the above categories this organisation will follow the relevant guidance currently available on the following website.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/

10. Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the organisation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

Subject access requests must be made in writing by letter or email to the DPO. They should include the name of the individual, correspondence address, contact number and email address and details of the information requested.

If staff receive something that may form a subject access request they must forward it to the DPO without delay. All requested information shall be provided within 1 month, except in the case of complex requests which justify an extension to 3 months. Individuals will be notified of any extensions to this period and why the extension is necessary as is practicable.

Before responding to a subject access request the organisation will need to verify the identity of the requesting individual. We will require 2 forms of identification, including passport or driving license ID as well as proof of address (e.g. bank statements, utility bills). Delays in providing the above may lead to extension of the response period.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May contact the individual via phone to confirm the request was made
- Will provide the information free of charge

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11. Biometric recognition systems

Where we use staff biometric data as part of an automated biometric ID system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Where staff members or other adults use the organisation's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and we will delete any relevant data already captured.

13. Photographs and videos

As part of our organisational activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers, or care users and learners aged 18 and over, for photographs and videos to be taken of them for marketing and promotional materials.

Where we need consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and care user or learner. Where we don't need parental consent, we will clearly explain to the care user or learner how the photograph and/or video will be used. Uses may be within the organisation on notice boards and in brochures, school newsletters, etc or on the website.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Data security and storage of records

The organisation will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. The ways in which we will ensure this are outlined in the *Information Security* policy.

In particular:

- Portable electronic devices, such as laptops and hard drives that contain personal data are password protected and automatically lock after the lowest possible period of inactivity

- Paper-based records containing personal data are kept in pseudonymised files, under lock and key, with only prescribed senior staff having access.

- Papers containing confidential personal data must not be left on office and classroom desks, on tables, pinned to notice/display boards, or left anywhere else where there is general access

- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals

- Currently, the organisation does not allow the use of removable media to move files containing personal information. If this becomes necessary, encryption software will be used to protect all removable media, such as USB devices, and the staff must destroy the information in accordance with this policy as soon as it is no longer required.

- All internal and external emails to professionals containing personal information shall be sent through encrypted means

15. Disposal and destruction of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

16. Retention periods of information

The organisation shall ensure it complies with relevant legislation (e.g. The Limitation Act 1980), statutory guidance (*Keeping Children Safe in Education*) and guidance provided by the Information and Records Management Society (IRMS) with regards its retention of information and shall dispose of records securely following the retention period for files and records of its type. The periods for some key information are included here, for an exhaustive list, see the link below.

- Child protection information, pupil education records, special educational needs files and reviews, individual education plans shall be retained for 25 years from the date of birth of the care user or learner, and then reviewed. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record.

- Minutes of Senior Leadership meetings, reports and records created by the Management Team or Senior Leadership shall be retained for 3 years from the date of the plan/report. Professional Development Plans and Home and School Development Plans shall be retained for the 'life' of the plan plus 3 years.

- School copies of curriculum management files and examination records shall, for the most part, be retained for 6 years from the date of entry or date of the exam.

IRMS Information Management Toolkit for Schools:
https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

17. Personal data breaches

The organisation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in *appendix 1*.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in our context may include safeguarding information being made available to an unauthorised person, or the theft of a laptop containing non-encrypted personal data.

18. Training

Data protection will also form part of continuing professional development, where changes to legislation, guidance or our processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full board of Directors.

20. Related Policies:
Information Security policy
Acceptable Use policy
Pictures and Internet Use Policy
CCTV Code of Practice

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the line function manager or head teacher and the board of directors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.

Appendix 2: Guidance relating to lawful bases for processing

Consent

The GDPR sets a high standard here. Consent means offering individuals real choice and control. Consent practices and existing paperwork will need to be refreshed and meet specific requirements. These are:

- Positive opt-in, no pre-ticked boxes or other method of "default" consent
- A clear and specific statement of consent
- Vague or blanket consent is not enough
- Keep consent requests separate from other terms and conditions
- Keep evidence of consent – who, when, how, and what you told people
- Keep consent under review
- Avoid making consent to processing pre-condition to any service
- Employers need to take extra care to evidence that consent is freely given, and should avoid over reliance on consent

Consent is one lawful basis to consider but organisations in a position of power over individuals should consider alternative "lawful bases". If we would still process their personal data without consent, then asking for consent is misleading and inherently unfair.

PLEASE NOTE
Consent within this policy relates only to data processing not Health or Support in a Social Care context. You must still use consent as defined within the relevant legislation to deliver services.

Legal Obligation

Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulations 2014), which requires us as providers to collect, handle and process data in a prescribed manner.

Legitimate Interests

This is the most flexible lawful basis for processing. It is likely to be appropriate where we process in ways that people would reasonably expect us to, with a minimal privacy impact, or where there is a compelling justification for the processing.

There are 3 elements to consider when using this lawful base. We need to:

- Identify a legitimate interest
- Show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms

Legitimate interests can mean ours, interest of third parties, commercial interests, individual or social benefits. The processing must be necessary. A balance must be struck between our interests, the individual's and would it be reasonable to expect the processing, or would it cause unnecessary harm, then their interests are likely to override our legitimate interests. You must keep a record of your legitimate interest's assessment (LIA) to help you demonstrate compliance.

The above are the 3 most pertinent bases for Health and Social Care data processing activity.

Contract, Vital Interests or Public Task apply within specific work settings and would be difficult to meet because service providers are subject to specific legislative and regulatory requirements in order to work within registered and regulated activities.

"Lawful bases" must be determined by the organisation before processing of any personal data and it is vital that thorough consideration is given to this decision.