Information and Data Security

Guidance for Knowsley Schools

Version 5.0

Version Control Record:

Revision	Date	Author	Summary of Changes
V1.0	19th November 2008	L Hornsby	
V2.0	18 February 2010.	Maria Bannister	
V3.0	18th March 2010	Maria Bannister	
V4.0	25th April 2013	Maria Bannister	Updated to include ICO guidance on legislative and technological changes.
V5.0	2019	Maria Bannister	Updated to include requirements under GDPR May 2018 and Data Protection Act 2018.
V6.0	2021	Karen Kelly	Updated following withdrawal from European Union

Version	Approved	Date
4.0	**Learning Technologies Strategy Board**	**25th April 2013**

Distribution: **Maintained Primary, Special and Secondary Schools**

Contents

1.0 INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) is a UK law which came into effect on 01 January 2021 and sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context,

The DPA 2018 sets out the framework for data protection law in the UK. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

The UK data protection regime takes a flexible, risk-based approach which puts the responsibility on data controllers to think about and justify how they use data. The data protection legislation is essentially about ensuring people can trust organisations to use their data fairly and responsibility. Loss of personal information can have significant implications for the school (data controller) including interruption of service delivery, financial penalties, loss of trust and reputational damage. For the person whose information has been lost (data subject) the implications can be even more significant including financial loss, emotional distress and in extreme cases even physical harm. The protection of information is not a discreet role – it is the responsibility of everyone who handles it. To ensure that information is adequately protected it is critical that the school creates a culture that properly values, protects and uses information appropriately. Information governance includes responsibility to ensure policies and procedures, performance measurement controls and reporting mechanisms to monitor compliance are in place and in operation across the school. Although the Principal or Head Teacher has ultimate responsibility as data controller they need to be supported in this by an information governance structure with clear lines of responsibility.

Knowsley Council is committed to ensuring the security of all information that it holds and implements the highest standards of information security in order to achieve this. This guidance is provided to schools to support them with the implementation of appropriate measures to ensure the appropriate handling of personal information.

2.0 SCOPE OF THE GUIDANCE

2.1 Schools are "data controllers" and are legally subject to the requirements of the UK GDPR and the Data Protection Act 2018. Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is not to be, processed. The UK GDPR covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of personal information. Collectively, these ensure the protection, integrity and appropriate access to and sharing of school information assets. These information assets may include information about current, past and prospective employees, pupils, suppliers, clients and others. This personal information must be dealt with

lawfully, correctly and in compliance with data protection legislation. This guidance is to support schools with these responsibilities and in doing so will ensure the protection of confidentiality, integrity and appropriate availability of school information assets.

2.2 The guidance has been provided to schools within the borough of Knowsley. Head Teachers and school governors are responsible for the adoption of the guidance, its implementation, subsequent compliance and ongoing review. Schools are responsible for ensuring that to all members of staff (including temporary workers), other contractors, volunteers, interns, governors and any and all third parties who have access to school information understand their responsibilities in ensuring the information is processed safely and in compliance with legislation.

3.0 DEFINITION OF DATA

3.1 Personal information is defined as any combination of information that identifies a living individual and provides specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth and so on, as well as other information such as academic achievements, other skills and abilities and progress in school. It may also include behaviour and attendance records. Data is any information, including electronic capture and storage, manual paper records, video and audio recordings. Any images, however created, are included. Schools hold personal information on learners, staff and other people to conduct day to day activities. Some of this information could be used by another person or criminal organisations to cause harm or distress to an individual or individuals. The loss of personal information could result in adverse media coverage and reputational damage and potentially legal action and financial sanction. Every member of your school, irrespective of their employment status (and others who are contracted to act as agents for the school) has a shared responsibility to secure any personal or sensitive information used in day to day professional duties. The secure handling of information is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to have proper controls in place makes the information, the data subject and the school as data controller vulnerable.

3.2 Special Category Data:

The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection – this is known as "special category data" and includes:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

The majority of the special categories are not defined and are fairly self-explanatory. However specific definitions are provided for genetic data, biometric data and health data. The UK GDPR

explains that these types of personal data merit specific protection because use of this data could create significant risks to the individual's fundamental rights and freedoms. For example, the various categories are closely linked with:

- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly and association;
- the right to bodily integrity;
- the right to respect for private and family life; or
- freedom from discrimination.

The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination. Whilst other data may also be sensitive, such as an individual's financial data, this does not raise the same fundamental issues and so does not constitute special category data for the purposes of the UK GDPR and while data about criminal allegations or convictions may raise some similar issues, it does not constitute special category data as it is covered by separate rules. However, you always need to ensure that when you are processing other types of data, it is fair and meets other UK GDPR requirements (including the separate rules on criminal offence data).

4.0 WHAT INFORMATION DO YOU NEED TO PROTECT?

Data protection legislation requires personal information, however it collected, used or stored, to be processed in compliance with the UK GDPR. This includes names, contact details, gender, date of birth and so on as well as sensitive information such as academic achievements, other skills and abilities and progress in school. It may also include behaviour and attendance records.

To ensure compliance with the legislation, schools should identify their information assets. These will include the personal information of learners and staff; such as assessment records, medical information and special educational needs information. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence. The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations. This information will form the Information Asset Register (IAR) which is a requirement of the "documentation principle".

5.0 THE ROLE OF THE INFORMATION COMMISSIONER

While the remit of the Information Commissioner (ICO) is broad, the main responsibility is to uphold information rights in the public interest: promoting openness by public bodies and data privacy for individuals. The duties include maintaining a register of controllers, monitoring compliance, handling complaints and providing support and guidance to organisations. The ICO has the power to take action against organisations - the maximum fine under UK GDPR is up to 4% of annual global turnover or £17.5 million – whichever is greater – for organisations that infringe its requirements. However, not all infringements lead to data protection fines and other penalities include issuing warnings and reprimands, imposing a temporary (or permanent) ban on processing, ordering rectification, restriction or erasure of data and suspending data transfers to third countries. The Data Protection (Charges and

Information) Regulations 2018 include the requirement for controllers to register with the Information Commissioner and pay the data protection fee.

6.0 The UK GDPR PRINCIPLES – Article 5 (1)

There are six key principles which are the foundation of the general data protection regime. These principles state that information must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals **('lawfulness, fairness and transparency'**);
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes **('purpose limitation');**
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation');**
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy');**
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar 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 implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals **('storage limitation');**
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality').**

In addition, Article 5 (2) adds that: "The controller shall be responsible for, and be able to demonstrate compliance" **('accountability').**

There is no principle for individuals' rights - this is now dealt with separately in Chapter III of the UK GDPR and there is no principle for international transfers of personal data - this is now dealt with separately in Chapter V of the UK GDPR. While these requirements are not covered by a principle, data controllers are still responsible for compliance.

The principles detailed above lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime and as such there are very limited exceptions. Failure to comply with the principles may leave organisations open to substantial fines. Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the UK GDPR.

7.0 DATA PROTECTION RIGHTS

One of the biggest changes from the previous data protection legislation relates to the rights of the individual (or data subject) as these have now been expanded. Previously, an individual could ask for

a school to produce a copy of all their data being held but now your school could be asked to delete all that data, produce it in a portable format or could withdraw any previously given consent.

Data subjects have the right to:

- be informed about how their data is being used
- access to their personal data (with some exemptions)
- have incorrect data rectified
- have data erased in certain circumstances
- stop or restrict the processing of their data in certain circumstances
- data portability (to get and reuse their data for different services) - this only applies if the processing is based on consent or provided as part of a contract and the processing is automated.
- object to how your data is processed in certain circumstances.

There are also specific rights about personal data being used for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

8.0 PUTTING THE PRINCIPLES INTO PRACTICE

To adequately protect information, organisations may need to make operational and technological changes. Some can be achieved quickly with existing resources; others will require extra investment and the help of IT and managed service suppliers. The information asset register will inform an information risk assessment of what needs to be done. Organisations may also need to make staff more aware of information security through training.
This section goes into more detail about the principles and measures schools need to take to ensure they are compliant.

8.1 **Principle (a)** is known as the **"lawfulness, fairness and transparency"** principle. It means that controllers must have legitimate grounds for collecting data and it must not have a negative effect on the person or be used in a way they wouldn't expect. Processing must be lawful, fair and transparent. This principle puts the requirement on schools to:

i. Identify valid grounds under the UK GDPR for collecting and using personal data.
ii. Ensure that you do not do anything with the data in breach of any other laws.
iii. Ensure that personal data is used in a way that is fair meaning you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
iv. You must be clear, open and honest with people from the start about how you will use their personal data.

Lawful: There are six valid lawful bases in order to process personal data and the most relevant will depend on the purpose and the relationship with the individual. Most lawful bases require that processing is "necessary" for a specific purpose. Controllers must determine the lawful basis for processing and include it in the privacy notice along with the purpose for processing. In the case of special category data, both the lawful basis for processing and an additional condition for processing must be identified.

The lawful bases for processing:

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Fair: Processing of personal data must be fair as well as lawful – if any aspect of the processing is unfair, this will be a breach of the principle even if you can demonstrate you have a lawful basis for processing. In general, fairness means that data should only be handled in the way that the subject would reasonably expect and that the processing does not have an unjustified, adverse affect on them. However, there may be circumstances where the processing negatively affects and individual with this necessarily being unfair.

Transparent: This is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about how any why you will use their personal data and you will need to included both the purpose for the processing and the lawful basis. You must ensure that you tell individuals about the processing in an accessible format ensuring that the language used is clear and plain.

8.2 **Principle (b)** is known as the **"purpose limitation"** principle. It means that personal data should only be collected for specified and explicity purposes and not used in a way that someone wouldn't expect. To be compliant with this principle you must:

- be clear about what the purpose for collecting the information and what will happen to it from the start
- comply with your documentation obligations to specify your purposes in a privacy notice for individuals from the start;
- comply with your transparency obligations to inform individuals about your purposes; and
- ensure that if you plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

8.3 **Principle (c)** is known as the **"data minimisation"** principle. It means that the data that is collected should be adequate (sufficient to properly fulfil the stated purpose), relevant (has a link to that purpose) and is limited to what is necessary (no more data than is necessary for the purpose is collected and stored). You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details. You must not collect or hold personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

8.4 **Principle (d)** is known as the **"accuracy"** principle. It means that controllers should take all reasonable steps to ensure that personal data held is correct and not misleading, that reasonal steps are taken to keep the personal data up to date, that reasonable steps are taken to correct incorrect or misleading information or to erase it as soon as possible and that any challenges to the accuracy of the personal data are carefully considered.

8.5 **Principle (e)** is known as the **"storage limitation"** principle**.** It means that personal data must not be kept for longer than is necessary and to ensure this is the case there should be a policy setting retention periods (wherever possible). There should be periodic reviews of data held and it should be erased or anonymised when it is not longer required. Any individual challenges to the retention of data must be carefully considered and individuals have a right to erasure if the information is no longer needed. Personal data can be retained for longer if it is being kept for public interest archiving, scientific or historical research for statistical purposes.

Storage limitation is important because ensuring personal data that is no longer needed is deleted or anonymised will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. In addition to complying with the data minimisation and accuracy principles limiting the storage of data reduces the risk of it being used in error. In addition, subject access request for personal data become more difficult to respond to if you are holding data for longer than is necessary.

Retention Periods: The DPA does not set out specific minimum or maximum periods for retaining personal data but principle (e) states that data should not be kept for longer than is necessary. You should have a Retention Policy which includes a retention schedule which states the type of record, what it is used for and how long it will be kept. A retention sechedule should form part of the "Information Asset Register" or processing documentation. The Records Information and Management Society is a useful reference when compiling a retention scheduled and information about how to contact them is included in the Useful Links Section.

Destruction of records: When it becomes necessary to destroy any printed or written documents containing personal, confidential and/or sensitive personal information, measures must be taken to ensure that it cannot be accessed by unauthorised parties in the future. Under no circumstances should personal, confidential and/or sensitive data be placed in general waste or recycling bins. Cross-cut shredders or confidential waste bins must be used for this type of information. Staff should be made aware of the arrangements for disposing of paper records. It is never acceptable to dispose of personal or special category data through domestic waste.

Deletion can mean different things in relation to electronic data and it may not always be possible to delete or erase all traces of the data. The key issue is to ensure the data is beyond use.

You must be able to justify why you need to keep personal data in a form that permits identification of individuals and if you do not need to identify individuals data should be anonymised so that individuals are no longer identifiable. You should also consider any regulatory requirements, relevant school standards and guidelines and whether the information is necessary to defend any future legal claims (unless there is some other reason for keeping it, information should be deleted when such a claim could no longer arise).

Remember, there is a significant difference between permanently deleting personal data and taking it offline. If data is stored offline, this should reduce its availability and the risk of misuse by mistake. However, it you still hold it, you must be prepared to respond to subject access requests for personal data stored offline and must comply with all the other principles and rights.

Data sharing: If you share data with other organisations, you should agree what happens once the need to share has ended. It may be that the information and any copies is returned or that all information is deleted using appropriate security. This requirement should be set down in an information sharing agreement that is agreed and signed by both parties.

8.6 **Principle (f)** is known as the **"integrity and confidentiality"** or **"security"** principle and it means that there must be appropriate security measures in place to protect the personal data held (manual or electronic) including having controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of records containing personal information. This includes things like risk analysis, organisational policies and physical and technical measures. This principle covers the sercurity of systems including confidentiality, intergrity and availability and measures to restore access to personal data in a timely manner in the event of a physical or technical incident. Measures to ensure that information is appropriately backed-up are critical to this and schools must ensure there is no single point of failure.

This principle also requires you to take account of additional requirements about the security of your processing, including the use of data processors. You also need to ensure that you have appropriate processes in place to test the effectiveness of the measures in place and undertake any required improvements. Schools must consider "the art of the possible" and costs of implementation when deciding what measures to take but they must be appropriate both to the circumstances and the risk your processing poses.

9.0 THE "ACCOUNTABILITY" PRINCIPLE

UK GDPR Article 5 (2) adds the "accountability" principle – this is a key principle and makes controllers not only responsible for complying with the UK GDPR but also demonstrating compliance. Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions. There are a number of measures that controllers can, and in some cases must, take including:

9.1 **adopting and implementing data protection policies including training and awareness raising**; The effective management of information is not a discreet role - it is the professional and moral responsibility of everyone who works in the school. It is therefore essential that the school leads from the top and that the provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities is given high priority. Training, alongside information governance and clear policies and procedures will ensure a culture where staff are able to access to the information they need, that the information is valued and that it is protected.

9.2 **taking a 'data protection by design and default' approach:** this is an integral element of being accountable. It is about embedding data protection into everything you do throughout all your processing operations. The UK GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features. Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in data protection impact assessments) demonstrates this.

9.3 **putting written contracts in place with organisations that process personal data on your behalf:** The UK GDPR makes written contracts between controllers and processors a requirement rather than just a way of demonstrating compliance. Whenever a controller uses a processor to handle personal data on their behalf, it must put a written contract in place that sets out each party's responsibilities and liabilities. Contracts must include certain specific terms as a minimum:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

9.3.1 **Responsibilitities on Controllers:** controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights. Controllers are primarily responsible for overall compliance with the UK GDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

9.3.2 **Responsibilities on Processors:** In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the UK GDPR. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures. A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to Article 28(3) must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

9.4 **Maintaining documentation of your processing activities, including written agreements and contracts as appropriate:** Article 30 of the UK GDPR contains explicit provisions about documenting your processing activities. This is important, not only because it is a legal requirement, but also because it supports good data governance and helps to demonstrate compliance. The obligations on controllers are:

- To document a record of the name and contact details of the school and your Data Protection Officer.
- The purposes for processing.
- A description of the categories of individuals and the categories of personal data.
- The categories of receipients of personal data (data sharing).
- Details of any transfers to third countiries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures
- Consent
- Any personal data breaches.

In addition, it is also useful to document information required for privacy notices such as the lawful basis for processing, the legitimate interests for processing, individual's rights, existence of automated decision making (including profiling) and the source of the personal data. You should also document:

- controller/processor contracts
- location of personal data
- Data Protection Impact Assessment reports
- Information required for processing special category data
- The condition for processing in the Data Protection Act
- The lawful basis for processing in the UK GDPR

Documentation can help you to comply with other aspects of the UK GDPR and improve your governance. In addition, you may be required to make the records available to the ICO on request. The records must be kept in writing, documented in a granular and meaningful way (most organisations will benefit from keeping the records electronically), kept up to date and reflect current processing activity.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as 'accountable' and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why. Accountability obligations are ongoing.

9.5 Implementing appropriate security measures:

Article 24(1) of the UK GDPR says "you must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR". The measures should be risk-based and proportionate and should be reviewed regularly and updated as required and link closely to Principle (f). You need to ensure the confidentiality, integrity and availability of the systems and services you use and the personal data you process with them. Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans. The UK GDPR does not specify an exhaustive list of things you need to do and it is not possible to include detail of every aspect of protection in this guidance but particular consideration should be given to the following areas:

9.5.1 Biometric Data: Article 9(1) includes biometric data in the list of special categories of data and Article 4 (14) defines this as "'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". The term 'dactyloscopic data' means fingerprint data. If you use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, you need to comply with the conditions listed in Article 9 – specifically:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

In addition, The Data Protection Act 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

9.5.2 Protective Markings: It is good practice to protectively mark personal information. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal information is included in a report and printed. There are different levels of marking depending on the information but as a guideline are 'official' and they should/could use a header or footer to denote this or a watermark on

templates. Anything with information about people is 'official personal sensitive and anything financial (procurement pre purchase) is 'official commercial'.

9.5.3 Access to Information and Access Control: Passwords are important in protecting information. Knowsley Council has implemented a complex password process which supports improved security on devices accessing the corporate network. It is important that passwords are easy to remember but hard to guess. It is good practice to have a password that has eight characters or more and contains upper and lower case letters, as well as numbers. Passwords must not be shared with anyone else, written down, used for personal online accounts or saved in web browsers. Passwords must never be emailed to someone else.

9.5.4 Device hardening: It is critical that your school network is protected against malicious virus attacks and the importance of having the right technical support in place cannot be under estimated. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Devices that connect to the Council's private (known as the 10) network must adhere to a set of security standards and it is the responsibility of the school to ensure that technical providers comply with these standards. Security features installed on devices should never be turned off or bypassed. It is also important that only approved and licenced software is installed and that any unused software is removed to remove security risks.

9.5.5 Email: Schools should ensure that staff are provided with an email account that is approved for school business and that the email provided has appropriate levels of security and meets UK GDPR requirements. Non approved emails should not be used for business purposes. The requirements governing the use of email should be included in an eMail Policy. Staff should be reminded that all emails that represent aspects of official business are the property of the business and not the individual.

9.5.6 Social Networking: Schools are well informed and proactive in promoting online safety and will have acceptable use policies in place. However, there are potentially problems with the emerging use of social media for business purposes including issues related to recruitment, selection and workplace monitoring. The blurring of social media for personal and business use is becoming particularly problematic and schools should review their Acceptable Use Policy to ensure it is explicit and clear about requirements. An alternative is to have a separate and specific Social Networking Policy which is reviewed regularly.

9.5.7 Websites: A website is the online showcase for the school and for many people is the first point of contact. The Department for Education has published a list of information that schools must include on their website and in addition it should also include the privacy notice and publication scheme – details of how to access information, and the contact information for the school Data Protection Officer.

Care should be taken before publishing information on the website and particular consideration should be given to safeguarding and data protection implications. General guidance includes:

- Do not disclose personal information – including images – without consent.

- On websites with controlled areas, ensure that the access is appropriately restricted (including removing access when it is no longer required) and strong password control is enforced.

- Be aware of metadata or deletions that could still be accessed in documents and images posted online.

Further information is available in the useful links section of this guidance.

9.5.8 Cookies: The rules on cookies are covered in UK GDPR regulation 6.

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions. You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent (consent must be actively and clearly given).

As long as you do this the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, bear in mind that devices may be used by different people. If there is likely to be more than one user, you may want to consider repeating this process at suitable intervals. You may also need to obtain fresh consent if your use of cookies changes over time.

9.5.9 Photographs: Photgraphs taken for personal or recreational use are exempt from data protection legislation, for example, if a family want to record a school activity that involves their child, data protection legislation does not prohibit them from doing so but the school may have a policy in place to prevent this for safeguarding or other reasons. However, if the school want to record an activity to sell on to families, they must ensure they are complying with the legislation.

Photographs taken for official school use may be covered so pupils and students should be advised why they are being taken. UK GDPR says there needs to be clarity and accountability and if the school is relying on consent this should include:

- Use in and around school, in places that might be seen by visitors
- On the school website
- On social media
- In wider marketing materials used by the school

You do not have to get consent for every photograph if you have a generic photographic consent form that covers these areas as long as you make it clear to the individual providing consent that it can be withdrawn at any time.

Extra care is needed if the photographs to be published are of young children or if the individuals are to be named. Caution should always be exercised if the photographs are to be published on a website.

9.5.10 Network Storage: Even when encrypted, information stored on a laptop and removable media is vulnerable to accidental loss, theft or device failure. Information should, by default, be stored

on a networked drive or portal where it can be backed up, recovered and made available to the school. You must be able to "restore access and availability to personal data in a timely manner" – this is a requirement of Principle (f).

9.5.11 Cloud Computing: is defined as "access to computational resources on demand via a network". In relation to data protection, the issues aren't new. The security of the data, overseas transfer rules and outsourcing considerations still apply and the responsibility remains with the school as the data controller. It is essential that before schools enter into a contract that a thorough risk assessment in undertaken. Further information is available through the useful links section of this guidance.

9.6 Security of Mobile Technologies:

9.6.1 Laptops and other devices with similar functionalities: Laptops are now a standard tool in the workplace and other devices with similar functionalities are becoming increasingly common. It is essential that the devices and the information they contain are adequately protected.

Laptops and other devices (i.e. notebooks, UMPCs etc) are portable by design and in some cases easy to conceal increasing the risk of theft. It is therefore important that appropriate measures are taken to protect them and the information they contain. Staff must ensure that equipment is transported securely, is only used/stored in a secure location (and by secure means) and is not left unattended. If possible, a visible security lock should be used. It is also good practice to store paper information separately from electronic equipment – one is protected by encryption while the other isn't!

9.6.2 Encryption: Users should not remove or copy personal or sensitive personal information from the school unless there is a business need and all portable and mobile devices, including media, used to store and transmit personal information must be protected using approved encryption software. School staff laptops have been secured using corporately approved encryption software and staff can check by looking for a yellow padlock at the bottom left of the laptop screen. An unencrypted device is a security risk. School ICT Support will be happy to provide advice.

9.6.3 Removable media: hard drives and other removable media are subject to device failure, damage, loss and theft making the information on them vulnerable - they should only be used when there is no other alternative with information saved back to a network as soon as possible. To ensure business information is protected and remains available to the school it must always be stored on a secure central server rather than locally on a device of any type. Ensuring staff regularly store their work or back up devices to a central server will ensure that information isn't lost to the organisation. If it is absolutely necessary to use temporary storage devices these must be encrypted to FIPS 140 – 2 certification. Unencrypted storage devices should never be used for the storage or transport of personal, special category personal or confidential information. Remember: removable media devices are subject to failure, loss or theft and they should only be used when there is absolutely no alternative.

9.6.4 Asset Management: Schools should have processes in place for tracking work devices and ensuring they are signed out, used in accordance with policy and returned at the end of employment or when staff relocate. Devices must be appropriately cleansed prior to reissue.

9.6.5 **Disposing of redundant IT equipment:** deleting files or formatting the hard drive does not provide adequate protection because information can easily be recovered using freely available software. It is essential that equipment is protected by encryption and that any school own equipment is retrieved when staff leave employment or relocate. Redundant equipment must be disposed of through approved contractors who have provided a guarantee that they will be securely cleansed and have provided a written undertaking about the process. A receipt should be obtained for all devices handed over for disaposal and the school inventory updated.

9.6.6 **Bring Your Own Device (BYOD):** The use of personally owned devices (typically smart phones or tablet devices) for business purposes is subject to much discussion and while there are merits, safeguards need to be put in place. Personal devices may be used by other members of the family, typically do not benefit from encryption or other security controls and there is little, if any, control over the disposal or reallocation of these devices. Careful consideration needs to be given to the potential risks including:

- Where does the information reside?
- How is the information transferred?
- How is the device managed and controlled?
- How is the privacy of the data subject protected?
- How is information deleted and the device disposed of?
- How is compliance with policy managed?

The issues aren't new but the solutions need to be considered carefully and robustly applied. Schools should carefully consider and implement a robust security strategy and acceptable use policy before activating BYOD.

Remember: technical measures can only provide a level of protection - to ensure complete security there must be a school culture of information security underpinned by governance, policies, procedures and training.

9.7 **Recording and, where necessary, reporting personal data breaches;** Controllers must report certain types of personal data breach to the Information Commissioner within 72 hours of becoming aware of the breach (where feasible). If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. Additionally, the UK GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not. You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this.

In the case of an information security incident or breach it is important to act quickly to mitigate potential harm or distress to individuals. There are four key stages:

1. **Containment and recovery:** the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. **Assessing the risks:** you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. **Notification of breaches:** informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as service providers, police and the banks; or the media.

4. **Evaluation and response:** it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly. It is also important that you have a procedure in place for dealing with any incidents and/or circumstances that do not result in breach, but could if they are not dealt with. KMBC Internal Audit Department can support you with this process.

9.8 Carrying out Data Protection Impact Assessments (DPIAs) for uses of personal data that are likely to result in high risk to individuals' interests: A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake. A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests. When done properly, a DPIA helps you assess how to comply with the requirements of the UK GDPR, while also acting as documented evidence of your decision-making and the steps you took.

9.9 Appointing a Data Protection Officer: It is a requirement of UK GDPR (37) that a Data Protection Officer is appointed by every organisation that processes or stores personal data and for all public authorities. Each school must therefore have a Data Protection Officer who is responsible for working out exactly what information needs to be secured and for ensuring the measures are in place to do so. DPOs assist the school in monitoring internal compliance, advise and inform on data protection obligations, advise on Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisior authority. The DPO's tasks are defined in Article 39 as:

- to inform and advise you and your employees about your obligations to comply with the UK GDPR and other data protection laws;

- to monitor compliance with the UK GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;

- to advise on, and to monitor, data protection impact assessments;

- to co-operate with the supervisory authority; and

- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

DPOs must be independent, expert in data protection practice, adequately resourced and report to the highest management level. The DPO cannot hold a position within the school that leads them to determine the purposes and means of processing personal data nor should the DPO

be expected to manage competing objectives that could result in data protection taking a secondary role to business interests. A DPO can be an existing employee or externally appointed and in some cases several organisations can appoint a single DPO between them. DPOs help to demonstrate compliance and are part of the enhanced focus on **accountability.** In addition, **Article 30** requires that organisations must maintain records of processing operations – a task that potentially sits best with the DPO. The DPO isn't personally liable for data protection compliance – this remains the responsibility of the data controller. However, the DPO clearly plays a crucial role in helping the orgainsiation to fulfil its data protection obligations.

9.10 Adhering to relevant codes of conduct and signing up to certification schemes:

The Data Ethics Framework (updated 30th August 2018) guides the design of appropriate data use in government and the wider public sector. This guidance is aimed at anyone working directly or indirectly with data in the public sector, including data practitioners (statisticians, analysts and data scientists), policymakers, operational staff and those helping produce data-informed insight. The Data Ethics Framework builds on the core values of the Civil Service Code - integrity, honesty, objectivity and impartiality - to encourage ethical data use to build better services and inform policy. A link to the document can be found in the useful links section.

10.0 BUILDING SECURITY AND CONTROL

There are of course technical measures that can be put in place to protect information but these will not work in isolation and must be underpinned by information governance, policies, procedures and training. Staff also need to be aware and continually vigilant to potential weaknesses that could pose a risk. Schools should ensure that regular checks are made of the physical security measures for the building (including access controls, locks, key register, alarms and CCTV) and that reception procedures for visitors are robust and adhered too.

11.0 CCTV

The ICO does not regulate the use of CCTV but does offer guidance because the use of CCTV involves the processing of personal information. If you use CCTV you must adhere to the ICO's Code of Practice for the use of CCTV. You do not need to ask individuals' permission to use CCTV, but you must make it clear where individuals are being recorded. Security cameras must be positioned carefully, clearly visible and accompanied by prominent signs explaining that CCTV is in use. Schools should have a CCTV Policy which covers the use of surveillance and CCTV systems which includes retention periods. CCTV images are covered by Subject Access Requests.

12.0 SHARING INFORMATION

There is a range of legislation that makes it a statutory responsibility to disclose/share information including: Children Act 1989, The Education Act 1996 (Sections 10 & 13) Crime & Disorder Act 1998, Youth Justice & Criminal Evidence Act 1999, Protection of Children Act 1999, Local Government Act 2000, The Learning & Skills Act 2000, Criminal Justice & Police Act 2001, special Education Needs & Disability Act 2001, Education Act 2002, The Children Act 2004 and The Data Protection Act 2018. This is not an exhaustive list and there will be other legislation that is applicable. Data Protection Legislation is not a barrier to appropriate and legitimate sharing of information and and in specific

circumstances one off sharing is appropriate where not doing so could result in harm. However, all sharing needs to be considered and the decision to share, or not, recorded.

Before any systematic sharing of personal or special category data with partner agencies care must be taken to ensure that the sharing meets the requirements of the UK GDPR and that an appropriate information sharing agreement is in place. The agreement needs to include details about how the information will be transferred and the measures that will be taken to protect the information including how long it will be retained. Schools should take precautions to ensure that legitimately shared information will be handled securely by the receiving organisations - they should not assume this will be the case – and information sharing agreements are critical because they set out the rules which each organisation agrees to work by, including keeping the information secure.

If a request is received to transfer personal information by any form of electronic means (including email, FTP and CD) the necessary encryption protocols need to be verified as in place. Information sent by fax is particularly vulnerable and this method should only be used when there is no other alternative and to not send the information would cause a serious disruption to service delivery or potentially result in harm. Schools should have a procedure in place for sending information by fax which mitigates the risk of information being compromised if it must be sent via this method. If a request is received to transfer printed or written personal, confidential and/or sensitive information, ensure that appropriate security procedures are in place, ideally a point-to-point courier with tracking and a signed receipt by the intended recipient. If a member of your staff is delivering personal information by hand, ensure they verify the identity of who they are handing it to and get a signature.

Schools should ensure that guidance is available on who they are allowed to share information with, how to share it securely and whether the information is shared systematically or as a one off.

12.1 Data Processing Agreements: The DPA is clear that where a data controller uses a third party (data processor) to process personal information on its behalf, a written contract (data processing agreement) must be put in place to ensuring the data processer has appropriate measures in place to ensure the safety and security of the personal information. The data controller must also take reasonable steps to ensure compliance by the data processor. It is the responsibility of the data controller to ensure that information processed by third parties on their behalf is dealt with according to the appropriate legislation and with integrity and that it is destroyed within appropriate retention periods.

12.2 Information Sharing Agreements: Information sharing agreements can take a variety of forms to support either systematic or ad hoc sharing and should be written to provide a framework and common understanding and agreement between parties sharing information. They should be clear, concise and relevant. Having an agreement in place does not indemnify against legal proceedings but it does demonstrate that measures have been taken to mitigate risk and ensure compliance and this would be taken into account by the ICO should they receive a complaint.

Having a clear understanding of what information should be shared, with who, when and how will ensure that schools collect and share personal information in compliance with the law, fairly, transparently and in line with the rights of the people whose information is being shared.

13.0 REQUESTS FOR INFORMATION

The UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 give rules for handling information about people including the rights of individuals to access their personal data. The Freedom of Information Act and the DPA 2018 come under the heading of information rights and are regulated by the ICO. The UK GDPR and the DPA 2018 exist to protect people's right to privacy, whereas the Freedom of Information Act is about getting rid of unnecessary secrecy. These two aims are not necessarily incompatible but there can be a tension between them, and applying them can require careful judgement.

When someone makes a request for information that includes someone else's personal data, you will need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. You will need to decide whether you can release the information without infringing the UK GDPR data protection principles.

13.1 Subject Access Requests:

Individuals have the right to access their personal data commonly referred to as a subject access request. Schools must make a record of such requests and responses, being careful to establish the identity of the individual making the request before releasing any information to them. They must also be careful to ensure that information about other individuals is not included in the response while providing as much information as possible to the requestor.

Individuals can make a subject access request verbally or in writing and you have one month to respond to a request (you can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual - you must let the individual know within one month of receiving their request and explain why the extension is necessary). Individuals have the right to obtain the following:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information:
- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;

- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

You may be providing much of this information already in your privacy notice.

In most circumstances, you cannot charge a fee to deal with a request, but you can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive or an individual requests further copies of their data following a request. You should base the reasonable fee on the administrative costs of complying with the request and if you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Subject access requests and children:

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them. Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

13.2 Freedom of Information Requests: The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

Anyone has a right to request information from a public authority and organisations receiving such a request have two separate duties: to tell the applicant whether they hold any information falling within the scope of their request; and to provide that information. **You normally have 20 working days to respond to a request**.

Any letter or email to a public authority asking for information is a request for recorded information under the Act. This doesn't mean you have to treat every enquiry formally as a request under the Act and in most cases you will can deal with a request for information (i.e. do you have space for a child) under routine procedures, but the provisions of the act must come into force if:

- you cannot provide the requested information straight away; or
- the requester makes it clear they expect a response under the Act.

To be valid under the Act, the request must:

- be in writing. This could be a letter or email. Requests can also be made via the web, or even on social networking sites such as Facebook or Twitter if your public authority uses these;
- include the requester's real name. The Act treats all requesters alike, so you should not normally seek to verify the requester's identity. However, you may decide to check their identity if it is clear they are using a pseudonym or if there are legitimate grounds for refusing their request and you suspect they are trying to avoid this happening, for example because their request is vexatious or repeated. Remember that a request can be made in the name of an organisation, or by one person on behalf of another, such as a solicitor on behalf of a client;
- include an address for correspondence. This need not be the person's residential or work address – it can be any address at which you can write to them, including a postal address or email address;

- describe the information requested. Any genuine attempt to describe the information will be enough to trigger the Act, even if the description is unclear, or you think it is too broad or unreasonable in some way. The Act covers information not documents, so a requester does not have to ask for a specific document (although they may do so). They can, for example, ask about a specific topic and expect you to gather the relevant information to answer their enquiry. Or they might describe other features of the information (eg author, date or type of document).

The Act contains other provisions to deal with requests which are too broad, unclear or unreasonable and you can ask for clarification.

A requester may ask for any information that is held by a public authority. However, this does not mean you are always obliged to provide the information. In some cases, there will be a good reason why you should not make public some or all of the information requested.

You can refuse an entire request under the following circumstances:

It would cost too much or take too much staff time to deal with the request.

The request is vexatious.

The request repeats a previous request from the same person.

In addition, the Freedom of Information Act contains a number of exemptions that allow you to withhold information from a requester. In some cases it will allow you to refuse to confirm or deny whether you hold information.

Some exemptions relate to a particular type of information, for instance, information relating to government policy. Other exemptions are based on the harm that would arise or would be likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests.

There is also an exemption for personal data if releasing it would be contrary to the UK General Data Protection Regulation (the UK GDPR) or the Data Protection Act 2018 (the DPA2018).

Even if a request is not valid under the Freedom of Information Act, this does not necessarily mean you can ignore You also have an obligation to provide advice and assistance to requesters. Where somebody seems to be requesting information but has failed to make a valid freedom of information request, you should draw their attention to their rights under the Act and tell them how to make a valid request.

There are a number of ways you could make information available, including by email, as a printed copy, on removable media or by arranging for the requester to view the information. When sending information electronically all documents must be converted to pdf format to ensure hidden data is not included. The exception to this is excel files however care must be taken to ensure no personal data is included. Normally, you should send the information by whatever means is most reasonable but requesters have the right to specify their preferred

means of communication in the initial request. Remember that disclosures under the Act are 'to the world', so anyone may see the information.

Your main obligation under the Act is to respond to requests promptly, with a time limit acting as the longest time you can take. Under the Act, most public authorities may take up to 20 working days to respond, counting the first working day after the request is received as the first day. For schools, the standard time limit is 20 school days, or 60 working days if this is shorter. Working day means any day other than a Saturday, Sunday, or public holidays and bank holidays; this may or may not be the same as the days you are open for business or staff are in work. The time allowed for complying with a request starts when your organisation receives it, not when it reaches the freedom of information officer or other relevant member of staff. Certain circumstances may allow you extra time (further guidance can be found on the ICO Website) but in all cases you must give the requester a written response within the standard time limit for compliance. Similiarly, there a limited circumstances in which you can refuse a request for example if it will cost more than £450 to find an extract the information. You must be clear as to the reason for refusal and notify the requester promptly.

Publication scheme:

The Freedom of Information Act 2000 (FOIA) requires all public authorities (including schools) to adopt and maintain a publication scheme (effectively a guide to the information they hold which is publically available) and a school will be in breach of the act if is has not adopted the ICO model publication scheme or is not publishing in accordance with it. Schools ared not required to inform the ICO that they have adopted the scheme – the assumption is that they have done so. A useful guide is available through the useful links section below.

14.0 MONITORING AND COMPLIANCE:

Schools must have an appropriate governance structure in place and ensure this is underpinned with appropriate and robust policies and procedures, training, technical controls and organisational processes. Training and awareness rising are critical to creating an organisational culture where information is valued and protected.

15.0 SUMMARY:

Loss of personal data can have significant implications for the school and for the person whose information has been compromised. Data protection legislation requires that organisations ensure that personal information is kept secure and the ICO has significant powers to sanction financially or issue an enforcement notice. There is also a risk of significant reputational damage. Schools must encourage a whole school culture where information is properly valued and protected and where each member of the school understands their professional and moral responsibilities. The information and guidance provided in this document supports schools in achieving and sustaining this objective.

REFERENCES:

The Information Commissioner plays a statutory role in policing compliance with the UK General Data Protection Regulation and the Data Protection Act 2018, and provides advice on relevant legislation and good practice. Extensive reference has been made to the information published by the ICO in the preparation of this guidance. www.ico.org.uk

USEFUL LINKS - FURTHER INFORMATION AVAILABLE FROM:

Information sharing: advice for practitioners providing safeguarding services to children, young people and carers. July 2018

Data Ethics Framework (August 2018)

ICO: Guide to Data Protection

ICO: Data Sharing Code of Practice

ICO: Guide to Freedom of Information

ICO: Guide to Right of Access

ICO: Employment Practices Guide
(note in Oct 2021 the ICO called for views on data protection and employment practice to shape new guidance)

ICO: Reporting a Breach

ICO: Publication Scheme - Guidance for Schools

ICO: Taking Photographs in Schools

Information Records Management Society: Toolkit for Schools

ICO: Guidance on the rules on use of cookies and similar technologies

ICO: Cloud Computing

ICO: Guidance on Accountability and Governance

ICO: Guidance on Individual's Rights

ICO: Guidance on Right to Erasure

ICO: Guidance on Special Category Data

Department for Education: Data Protection Toolkit for Schools August 2018