IPSWICH SCHOOL

DATA PROTECTION POLICY

The Data Protection Act 2018 (DPA18) is the UK's implementation of the General Data Protection Regulation (UK GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

The school as the Data Controller will comply with its obligations under the DPA 18. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner (ICO) as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the DPA 18, therefore it is imperative that the School and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the DPA 18 personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The 7 Principles of GDPR 18

The principles set out in DPA 18 must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the Compliance Officer if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

The following basis would apply to most of the School's Activities.

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

Any Staff member who wishes to process data (this includes obtaining new data) must ensure that this is agreed with the Compliance Officer, before any processing takes place.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interest assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified above
- One of the special conditions for processing sensitive personal information applies:

    (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    (e) the processing relates to personal data which are manifestly made public by the data subject
    (f) the processing is necessary for the establishment, exercise or defence of legal claims
    (g) the processing is necessary for reasons of substantial public interest
    (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
    (i) the processing is necessary for reasons of public interest in the area of public health.

The School's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. **Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the DPA 18.** (School Contract and the Annual Parental Data Capture Form etc.)

Data Protection Impact Assessments (DPIA) - Annex E

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

When carrying out a DPIA, staff should seek the advice of the Compliance Officer for support and guidance and once complete, refer the finalised document to the Compliance Officer for sign off.

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the School's record of processing activities the Compliance Officer will document, or link to documentation on:

- information required for privacy notices
- records of consent (Shared Drive)
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by DPA 18 including the identity of the Compliance Officer, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the DPA 18 as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the DPA 18 and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see Ipswich School privacy notices)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request.
- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but Ipswich School do not want the data to be erased) or where the school no longer need the personal information, but Ipswich School require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where Ipswich School do not think it is accurate (and the school are verifying whether it is accurate), or where Ipswich School have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintained in accordance with the DPA 18.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the Health, Safety & Compliance Officer.

Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations. (*Appendix A refers to the Schools Retention Policy)*

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.
Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager and the Compliance Officer immediately, that a data breach is discovered and make all reasonable efforts to recover the information, following the ICO breach reporting process.

If the Compliance Officer is not available they must report to the Director of Financial Operations or Head/Head Teacher(Prep).

Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's Compliance Officer.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to mrr@ipswich.school

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Queries and Complaints

Any comments or queries should be directed to the Compliance Officer using the following contact details:

GDPR
Ipswich School
25 Henley Road
Ipswich IP1 3SG
mrr@ipswich.school

M R Rackham, Compliance Officer, Ipswich School

Review date January 2025

Appendixes

A - Staff - Policy Summary
B - Retention Policy
    (i) Attachment - Table of retention
C - Individual Rights
D - LIA & DPIA
E - Profiling - Marketing
F - SAR Policy and procedures
    (i) Attachment - 5 Steps to SAR
    (ii) Attachment - Sample SAR Letters

Other Policies:

Ipswich School CCTV policy
Data Mapping - Held by mrr@ipswich.school
Exam Data Retention Policy
Ipswich School Privacy Notice

Appendix A

DATA RETENTION POLICY - SUMMARY FOR STAFF

General

Ipswich School Data Retention Policy forms an essential part of the personal data lifecycle. This Summary has been produced to remind staff of the key points and will be shared on the School shared drives.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

The following basis would apply to most of the School's Activities.

- Processing is necessary for the purposes of the legitimate interests of Ipswich School

Data Protection Principles

The Data Protection Act (2018) defines six Data Protection Principles; which all processors of personal information must abide by. The 6 principles are:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

There are also **stronger rights for individuals** regarding their own data.

The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

Definitions

Term	Definition	Example
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.	Register, Mark Book, email, SOS List etc.
Data controller:	The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be, recorded.	In our case, the Data Controller is Ipswich School
Data processor	Any person who processes data on behalf of the data controller.	You, Me etc.

Explicit consent	A form of consent normally given orally or in writing and is where a patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.	Parents Contract will include "Consent" where applicable, i.e. Media
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data.	

Staff Responsibilities and Guidance

Everyone working for the Ipswich School has a legal duty to keep information about Staff, Pupils, Parents and other individuals such as Alumni or volunteers confidential. They are required to adhere to school policies, contract of employment etc.

In the course of your employment you will have access to personal information relating to the School, its Pupils, parents, employees, other parties, as well as information relating to the School's policies or finances. You must not use such information for your own benefit nor disclose it to other persons without the consent of the School and the party concerned unless required to do so by law. This applies both during and after the termination of your employment. If any member of staff is found to have revealed information without consent, disciplinary action may be taken. If you are in any doubt regarding the use of information in the pursuit of your duties, you should seek advice from SMT or the Health, Safety and Compliance Officer before communicating such information to any third party. Nothing in this clause inhibits the provisions of the Public Interest Disclosure Act 1998.

Breach of Policy and Procedure

Any breach of data protection and confidentiality can have severe implications for the School, its pupils, parents and staff.
The office of the Information Commissioner's Office (ICO) regulates data protection and is charged with upholding an individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to £20,000,000.

Staff who wish to report incidents relating to data protection act should contact GDPR@ipswich.school

Dos & Don'ts:

DO:

1. Use strong passwords – at least 8 characters, with upper and lower-case letters and special characters
2. Regularly 'cleanse' the information you hold, and dispose of anything you no longer need
3. Send and save scanned files to a secure folder that only authorised people can access (Google Drive)
4. Turn off the 'autofill' function on your emails, to reduce the risk of emailing the wrong person
5. Double-check that you're sending information to the correct person, who has the right to view it
6. **Use "bcc" when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents**

7. Keep personal data anonymous where possible
8. Think before you put information up on the wall ...
    - Do you have a good reason to display it?
    - Do you need consent from the parent or pupil?
    - Might there be a safeguarding risk in displaying it?
    - Read and understand all of the school's policies on data protection
    - Report safeguarding concerns to the relevant people where you're concerned about a child – data protection laws **DO NOT** stop you from doing this
    - Only collect information about pupils and parents/carers that you actually need
    - Keep data in a safe place when taking it home

DON'T:

1. Write passwords down anywhere
2. Leave personal data unattended:
    - On your desk
    - On an unattended computer screen
    - On top of the printer
    - Anywhere else someone might see it when they aren't supposed to
    - Take any sensitive or confidential personal information home with you
    - Use a memory stick. If you really need to, make sure it's encrypted/password protected.

Appendix B

DATA RETENTION POLICY - IPSWICH SCHOOL

Overview

A Data Retention Policy forms an essential part of the personal data lifecycle. Data shall be maintained for as long as there is an operational need. The length of time it will be retained will be set out in the Data Retention Schedule.

Purpose

This policy addresses the requirements surrounding Data Retention as set out by the DPA 18 and how Ipswich School meets its obligations to individuals and the law regarding the retention of personal data.
This document serves to inform all staff members who process personal data on behalf of the School. The purpose of this policy is to:

- minimise the retention period of records while ensuring that the information needs of the business are met
- ensure that records required for legal and evidential purposes are kept for the appropriate period and in an appropriate manner
- ensure that records are not destroyed prematurely

We need to do this in order to:

- ensure the School complies with the law
- protect staff and other individuals
- protect the organisation

Scope

This document applies to the retention of personal data, which is processed and subsequently retained by the School. It should be read in conjunction with the **Data Retention Schedule** which specifies retention periods for each type of data. It applies to all staff, contractors and temporary employees who hold or process any the School records for any purpose. It applies equally to our own servers, third party servers, email accounts, backup storage such as photographic, microform and electronic media that are used to store records as well as to more traditional paper or card records.

Policy

- Personal data shall not be kept for longer than is necessary for a given purpose. However, the retention period can differ based on the type of data processed
- The Data Retention Schedule lists the types of personal data maintained by the School and specifies the Retention period for each data type. If the School acquires a new type of data, the Data Retention Schedule must be updated accordingly.
- No records involved in any investigation, litigation or audit will be destroyed until legal counsel has confirmed that no further legal reason exists for retention of the record. It is the responsibility of senior management involved to ensure related documents have been segregated appropriately.

Storage Guidelines

A document should not normally be stored both on paper and electronically, nor stored electronically in several different locations; a single electronic version (stored so as to be accessible, Google Drive, to all who need the information it contains) is preferred. There may be some exceptions to this, for example, exam-related paperwork referring to candidate enrolments, results and/or reports where we may take a scanned copy for ease of access to the information but where we also need to keep the original for purpose of checking signature or other hand-written details.

Retention Periods

Specific retention periods are detailed in the **Data Retention Schedule**. Where there is a statutory retention period for a record, this will be treated as a minimum period. No information should be kept indefinitely 'just in case'. In terms of information obligations, data subjects must be informed of:

- The retention period;
- If no fixed retention period can be provided – the criteria used to determine that period; and The new retention period if the purpose of processing has changed after personal data has been obtained

After the retention period has expired, the personal data does not necessarily have to be completely erased. In line with the School's Data Destruction Policy it is sufficient to anonymise the data, for example, by erasing single pieces of information that identify the data subject (whether alone or in combination with other pieces of information). In cases where the data cannot be allocated to an identifiable person, no action will be required.

Ipswich School

Table for Storage and Retention of Records and Documents

The purpose of a retention table is to inform staff of the length of time which a record needs to be kept. It means that members of staff can be confident about destroying information at the appropriate time. Where records have been identified

Where records have been identified for destruction they should be disposed of in an appropriate way. Some sensitive information may require shredding before disposal.

Transferring to Archives is designed for those records that have been identified as worthy of permanent preservation, arrangements should be made to transfer the records to the Archives.

Type of Record/Document	DATA	Retention Period
SCHOOL-SPECIFIC RECORDS		
DfE Registration documents of the School		Permanent (or until closure of the school)
Attendance Register	ISAMs	7 years from the last date of entry.
Minutes of Governors' meetings	Google drive	Archive Google
Annual curriculum	ISAMs, Google	From end of year: 3 years (or 1 year for other class records: e.g. marks/timetables/ assignments)
PARENTAL CONTRACTS AND AGREEMENTS		
Assessments, records of decisions relating to Admissions	Admissions Archive	25 years from date of birth
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Bursary as per Financial Regulations	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Examination results (external – GCSE, A Level)	ISAMs	7 years from pupil leaving school
Examination results (internal, i.e. Mocks, Prep Exams)	Also see Exams Retention Policy	1 Year
INDIVIDUAL PUPIL RECORDS		**NB – this will generally be personal data**
Admissions: application forms, Nursery (Lodge)	Registrar & Admissions Archives	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
Prep Data	Target Tracker / SONAR	
Pupil file including:		ALL: 25 years from date of birth (subject

		where
Pupil reports	Pupil Archives	relevant to safeguarding considerations
Pupil performance records	ISAMs	Any material which may be relevant to potential claims should be kept for the lifetime of the pupil)
Pupil medical records		
Special educational needs records (to be Risk Assessed individually)	SEN Lead	Date of birth plus up to 25 years (allowing for special extensions to statutory limitation period)
Pastoral Meeting Notes	Head's / Prep Headteacher Archive	7 years from pupil leaving school unless incident which should be kept as child protection files/ incident reporting
Early Years Funding records	Prep / Bursar Archive	7 years
Trip Letters and Consent	Google Archive	7 Years from Cohort leaving
		(As of 2019, all Paperwork electronic – IS Post)
Alumni Past/Present Records	OI Archive	Current Academic Year Lifetime of Alumni/Past parents (Subject to Consent or legitimate interest)
Contact Details		
Communication Records		
SAFEGUARDING		
Policies and procedures	school Archive	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	Bursary	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
Accident / Incident reporting	Matron Paper Copies (Electronic Google) RIDDOR	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
Child Protection files	DSL(s)	If a referral has been made / social care has been involved or the child has been subject of a multi-agency plan – **indefinitely.**
Low-level concerns	DSL / HR	Low-level concerns apply to the conduct of adults working in schools with children. These concerns are about behaviour that is inconsistent with the School's code of conduct,

		but is not serious enough to be referred to the local authority.
ACCOUNTING RECORDS		
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state)	Bursary as per Financial Regulations	Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
Tax returns	As above	Minimum – 6 years
VAT returns	As above	Minimum – 6 years
Budget and internal financial reports	As above	Minimum – 3 years
Bursary Applications	As above	
SUPPLIER CONTRACTS AND AGREEMENTS		
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Bursary as per Financial Regulations	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Bursary as per Financial Regulations	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS		
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	School Archive	Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise expiry of right plus minimum of 7 years.
Assignments of intellectual property to or from the school	School Archive	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	School Archive	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS		NB this will contain personal data
Single Central Record of employees Contracts of employment	Bursary as per Financial Regulations	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself - 6 months as above)
Employee appraisals or reviews	HR	7 years from effective date of end of contract Unless there are concerns. HR to review (HR & Safeguarding)
Staff personnel file	HR	Duration of employment plus minimum of 7

		years
Payroll, salary, maternity pay records	Bursary	Minimum – 6 years
Pension or other benefit schedule records	Bursary	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	HR	Minimum 3 months but no more than 1 year
Health records relating to employees	HR	7 years from end of contract of employment
INSURANCE RECORDS		
Insurance policies (will vary – private, public, professional indemnity	Bursary	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
ENVIRONMENTAL & HEALTH RECORDS		
Maintenance logs	Bursary as per Financial Regulations	10 years from date of last entry
Accidents to children	Matron	25 years from birth (unless safeguarding incident)
Accident at work records (staff)	Matron & HR	Minimum – 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances	H&S	Minimum – 7 years from end of date of use
Risk assessments (carried out in respect of above)	Google shared Drive	7 years from completion of relevant project, incident, event or activity.
Data Protection Records documenting processing activity, data breaches	HR	No Limit- as long as upto date and relevant and contains no personal data

APPENDIX C

INDIVIDUAL RIGHTS

The Data Protection Act. Below are the 8 main rights and a brief explanation of each one to give you a better understanding. (follow links for more information)

1. The right to be informed
The right to be informed states how the information Ipswich School supply about the processing of personal data must be, typically in a privacy notice:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

2. The right of access
Under the right of access, Ipswich School must be able to provide processing confirmation and access to an individual's data free of charge and provide it in a commonly used format - an electronic format if the request is made electronically.

3. The right to rectification
Individuals are entitled to have their personal data rectified if inaccurate or incomplete and Ipswich School must respond to a rectification request within one month if not deemed complex. Ipswich School must inform related third parties where possible if the personal data is disclosed to them also.

4. The right to erasure
'The right to be forgotten', or right to erasure means Ipswich School must have procedures in place for removing or deleting personal data easily and securely where there is no compelling reason for possession and continued processing. Specific circumstances stated by the include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the UK GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Especially for marketing, this right is a main reason why having the appropriate tools and record keeping in place is so important to know why someone's data is being processed and what it relates to, and if someone has removed their consent to receiving marketing materials and having their data processed. Many investigations will likely arise through people being disgruntled when they have withdrawn their consent from marketing materials, or not given their consent initially for marketing materials, but are still being processed and receiving electronic marketing such as emails for example.

5. The right to restrict processing
Individuals have the right to 'block' or restrict processing of personal data, in the following circumstances outlined by the ICO:

- "Where an individual contests the accuracy of the personal data, Ipswich School should restrict the processing until Ipswich School has verified the accuracy of the personal data."
- "Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and Ipswich School are considering whether the organisation's legitimate grounds override those of the individual."
- "When processing is unlawful and the individual opposes erasure and requests restriction instead."
- "If Ipswich School no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim."

Ipswich School must inform any third parties that are also involved with the data about the restriction, and inform individuals when Ipswich School removes a restriction on processing.

6. The right to data portability
The right to data portability allows individuals to obtain and reuse their personal data across different services for their own purposes. The right only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is automated.

Personal data must be provided in a structured, commonly used and machine readable format (like CSV files) so other organisations can use it, and must be provided free of charge.

7. The right to object
The right to object means individuals have the right to object to direct marketing (including profiling), processing based on legitimate interest, and purposes of scientific/historical research and statistics, in which case Ipswich School must stop processing personal data immediately and at any time, with no exemptions or grounds to refuse, free of charge.

Ensure Ipswich School are informing individuals of their right to object in their privacy notice and "at the point of first communication".

8. Rights related to automated decision making and profiling
If any of your processing operations constitute automated decision making including profiling (such as insurance firms), individuals have the right not to be subject to a decision and must be able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it. The right does not apply if the automated decision is a contractual necessity between Ipswich School and the person, if it's authorised by law, or if based on explicit consent.

APPENDIX D

Ipswich School LIA

This legitimate interest's assessment (LIA) template is designed to help you and the Compliance Officer to decide whether or not the legitimate interest's basis is likely to apply to your processing.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative? • Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
Likely impact
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests' basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

Data Protection Impact Assessment (DPIA)

Under DPA 18 there is a greater focus on actively managing the risks around processing personal data. Part of this management is the completion of Data Protection Impact Assessments (DPIAs). These act rather like most risk assessment exercises; encouraging people to look carefully at what they are doing, why they are doing it, the risks involved and controlling those risks to an acceptable level.

Under DPA 18 DPIAs must in accordance with Article 35 be completed where the use of the data "is likely to result in a high risk to the rights and freedoms of natural persons". The risks can arise from the activity and the category and quantity of the data to be used.

Step 1

Identify if a DPIA is needed

1) It might be helpful to answer screening questions to identify a proposal's potential impact on privacy, consider in particular:

   - Are new technologies being used?
   - Will the proposal involve automated decision making or profiling?
   - Are special categories of personal data being processed?
   - Is a large volume of personal data being processed?
   - Will the proposal involve the systematic surveillance of large public spaces?
   - Are datasets being merged?
   - Is the personal data of vulnerable individuals being processed?
   - Is data being transferred outside the EU?
   - Will personal data be processed in ways which individuals might not reasonably expect?

2) If you think it likely that a DPIA is required contact the Compliance Officer who can provide guidance.

Step 2

Determine that the processing is necessary and proportionate

3) Describe the processing that is being proposed and why it is being proposed; this will include an analysis of how the data will be obtained, used and retained.

4) Assess the necessity and proportionality of the processing in relation to the purpose, i.e. can it be done another way that requires less processing of personal data?

5) Always consider whether you can anonymise or at least pseudonymise the data you wish to process. You may be able to anonymise at a later date, safely destroying the original identifiable data. Also consider whether you can conduct the activity with less data either in terms of quantity or quality – only take what you need.

Step 3

Identify the risks associated with the processing

6) You will need to assess the risks to the rights and freedoms of the individuals whose data is being processed, i.e. what would happen if the data was lost or misused in some way? This needs to include consideration of the rights afforded to individuals under the DPA 18.

See ICO guidance:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-GDPR/individual-rights/

7) Also consider the risk that the processing poses (if any) to compliance with the DPA 18 and to the school more broadly.

   The following table can be used:

Proposed processing	Risk to individual	Compliance risk	Associated organisation risk

Step 4

Identify solutions/mitigations to the risks

8) Describe safeguards and security measures put in place, privacy by design, use of data processing and data sharing agreements.

9) Consider seeking the views of the data subjects, or their representatives and other interested parties (i.e. data processors, sector specialists).

Step 5

Document the findings

10) The following table can be used:

Risk	Solution	Result (is the risk eliminated, reduced or accepted?)	Evaluation: is the final impact on individuals justified, compliant and proportionate?

Step 6

Feed the results into the proposal

11) Assess if there are changes that need to be made to the proposal, and define how the risks will be monitored.

12) Make sure that the solutions proposed deal with the risk. If you are not sure about acceptable levels please contact the Data Protection Officer.

Step 7

Implementation

13) Once you have completed the above findings and it is safe to proceed make sure that all those involved in the processing are aware of the necessary solutions.

14) Regularly review processing activity to make sure it is still compliant with the acceptable position and be responsive to any necessary changes.

APPENDIX E

DPA 18 - AUTOMATED DECISION MAKING AND PROFILING

DPA 18 introduces specific controls in relation to certain kinds of automated decision making and profiling.

This guide provides an overview of what is changing and how it will be interpreted by supervisory authorities, such as the UK's Information Commissioner (ICO).

What is automated decision making and profiling?

Automated decision making and profiling are two separate, but often interlinked concepts.

a. **Profiling** is a form of automated processing of personal data used to analyse or predict matters relating to an individual. For example analysing an individual's performance at work, financial status, health, interests or location.
b. **Automated decision making** is the ability to make decisions without human involvement. In practice, profiling can often be a precursor to automated decision making.

Profiling and automated decision making can be used in three ways:

a. General profiling - Individuals are segmented into different groups based on data analysis
b. Decision making based on profiling - A human makes a decision based on profiling
c. Solely automated decision making - An algorithm makes a decision with no human input

General prohibition on certain types of automated decision making

Prohibiting decisions based solely on automated decision making which produce legal effects or similarly significantly affect an individual unless:

- It is necessary for the performance of or entering into a contract;
- It is authorised by law; or
- It is based on the data subject's explicit consent.

Automated decision making that involves special categories of personal data, such as information about, health, sexuality, and religious beliefs, is only permitted where it is carried out on the basis of explicit consent or where it is necessary for reasons of substantial public interest, such as fraud prevention and operating an insurance business.

Necessity is interpreted narrowly, and organisations must be able to show that it is not possible to use less intrusive means to achieve the same goal.

As with general consent under the DPA 18, any consent must be freely given, unambiguous, specific and informed.

What is meant by 'legal effects' or 'similarly significant effects'?

'Legal effects' are things that have an impact on an individual's legal rights or affect a person's legal status or rights under a contract. Examples include:

- Being entitled or denied benefits such as housing or child benefit
- Being refused entry at a national border
- Automatic disconnection from a mobile phone service because an individual forgot to pay their bill

'Similarly significantly affects' means decisions that have non-trivial consequences, such as:

- Automatic refusal of an online credit application

- Automated decisions about credit limits, based on analysis of spending habits and location

What do I need to tell individuals?

Where decisions are made solely using automated decision making, organisations must:

- tell the individual that it is using automated decision making for these purposes;
- provide meaningful information about the logic involved (for example by explaining
- the data sources and main characteristics of the decision making process); and
- explain the significance and envisaged consequences

The Article 29 Working Party recommends that these steps are followed whenever automated decision making is used, as this can help with ensuring that the processing is carried out fairly.

Safeguards and transparency

Individuals must be told when a decision has been taken solely using automated decision making and they must have the right to request a review of the decision. The review should be .by a person with appropriate authority and capacity to change the decision and should involve a thorough review of all relevant information.

Organisations using automated decision making should also carry our regular reviews and use appropriate procedures to prevent errors.

APPENDIX F

Subject Access Request (SAR) Policy & Procedure

SCOPE

The following procedure describes the procedure to be followed when handling Subject Access Requests received by the Ipswich School (the Data Controller) under the Data protection Act 2018 (DPA18)

RIGHT OF ACCESS TO PERSONAL DATA

Under DPA 18 an individual has the right to access their personal data processed by the Data Controller (i.e. Ipswich School), specifically an individual is entitled to:

a) Be informed by Ipswich School whether personal data of which they are the data subject are being processed by or on behalf of the school.
b) Be given a description of that data, including the personal data of which the individual is the data subject, the
    a. purpose for which the data are being or are due to be processed and the recipients or classes of recipients to whom
    b. the data are or may be disclosed.
c) Have communicated to them in an intelligible form the information constituting any personal data of which that
    a. individual is the data subject, any information available to the school as to the source of those data, and where the
    b. data is used for the purpose of evaluating matters that has constituted or is likely to constitute the sole basis for any
    c. decision significantly affecting them (e.g. performance at work, their conduct or creditworthiness), to be informed
    d. by the school of the logic involved in that decision-taking.
d) Verify the lawfulness (Legitimate Interest) of the processing of their personal data.

DEFINITION OF PERSONAL DATA

Personal data means any information that relates to a living individual who can be identified

HOW TO OBTAIN ACCESS TO YOUR PERSONAL DATA: THE SUBJECT ACCESS REQUEST PROCEDURE

In order to obtain access to your personal data, you must make your request in writing. This is known as a Subject Access Request (SAR). You may make an SAR by contacting GDPR@ipswich.school

Your written request should include the following information to enable us to process it efficiently:

a) Sufficient information to identify yourself to prevent unauthorised disclosures to third parties, e.g. any relevant reference numbers or account numbers, dates of correspondence and details of employees you have dealt with, etc.
b) The information you are seeking. Where a request is made by an agent on your behalf, in addition to the above, a request will only be fulfilled where the agent can provide proof of authority to act on your behalf.

It is important to note that a data controller is not obliged to comply with a request until they are provided with sufficient information necessary to confirm your identity and to locate the information you seek, so it is important to provide this information from the outset.

INFORMATION CONTAINING PERSONAL DATA ABOUT THIRD PARTIES

Some information within your request may contain personal data related to other individuals (third parties). Your request may therefore lead to a conflict of interest between your rights to this information and the third party's rights regarding their own personal information. In order to ensure that the data of third parties is not compromised. Ipswich School shall redact or edit (e.g. provide excerpts of information) information so that third parties' data does not form part of the requested information.

CHARGING A FEE FOR / REFUSING TO RESPOND TO SUBJECT ACCESS REQUESTS

In line with the DPA 18 the UCO will fulfil all SAR's free of charge, however, where a request is either manifestly unfounded or excessive, particularly if it is repetitive we may:

a) Charge a reasonable fee taking into account the administrative costs of providing the information; or
b) Refuse to respond.

APPEALS PROCEDURE

Ipswich School has the established appeals procedure to provide individuals the opportunity to request an internal review of their SAR outcome. This procedure shall:

a) Reassess the way in which the request was handled and provided.
b) Be undertaken by senior and impartial staff members able to make an independent decision that may overturn the original outcome if required.

Requesters may not be satisfied with the outcome of their request for the following reasons:

a) Disagree with our interpretation of their request.
b) Believe we hold more information than we have disclosed.
c) Still be waiting for a response and are unhappy with the delay.

If a requester is not satisfied with the outcome of their request they should write to the Bursar or email mrr@ipswich.schoo lto request an internal review explaining why they are dissatisfied with the outcome or handling of their request within 60 days of receiving their initial outcome:

Attachments:

1. Dealing with an SAR - **The 5 Steps** & Flow CHart
2. Sample SAR Letters
3. SAR Log

Attachment 1 - Dealing with an SAR - **The 5 Steps**

Step One: Initial Steps

- SAR recorded on the SAR Log (attachment 2 to Annex F, Data Protection Policy)
- SAR made by the data subject or someone the data subject has authorised to make the SAR on their behalf. (evidence of authority to be obtained)
- ID Has been Provided or is not required
- Sufficient Information has been provided to enable the relevant personal data to be located
- Response date calculated and acknowledgement and request for further information sent to data subject
    -

Step Two: The Search

- All relevant paper files have been identified and searched
- All relevant electronic files have been identified and searched

Step Three: The Document Review

- All Non-Personal data removed or decision made to disclose
- All 3rd party data identified and, either:
    - Disclosed (3rd party consent)
    - DIsclosed (Reasonable to disclose without consent)
    - Removed or Redacted

Exemptions considered and applied where appropriate

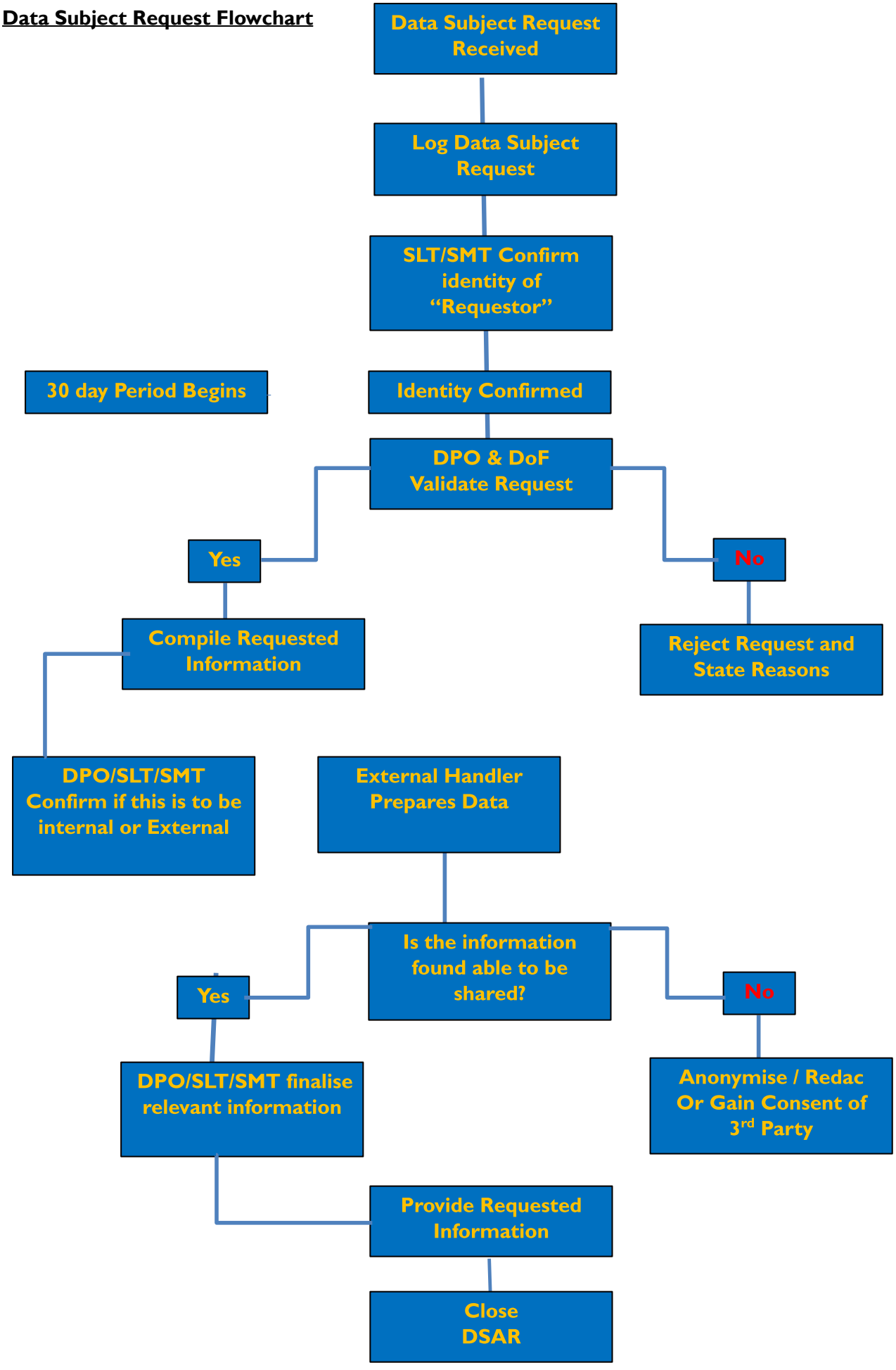
Step Four: The response

- Disclosable personal data compiled and checked
- Cover letter prepared covering:
    - Article 15
    - Confirmation of whether personal data has been disclosed ib full or withheld in whole/part and, if so, on what basis disclosure has been refused and the individuals rights to complain to the ICO or seek judicial remedy.
    - an explanation of any codes or complex terms contained within the information disclosed
- Appropriate and secure delivery method (Signed for, by hand etc.)

Step Five: Housekeeping

- Details of the SAR added to the SAR Log
- Decisions made recorded
- Copy of full response retained

Data Subject Request Flowchart



Attachment 2 - Sample Letters

Letter One - **Acknowledgment of Request**

Name (Requester)
Address

Date:

Dear XXXXX

Reference: Subject Data Request XX

We write to acknowledge receipt of your request dated DD/MM/YYYY made under Data Protection Regulations. We received your request on DD/MM/YYYY.

The DPA 18 requires us to respond to requests within one month of receipt. We expect to provide you with a response by DD/MM/YYYY. However in certain circumstances, the DPA 18 or other applicable law allows us to extend that deadline by two months, depending on the complexity of your request. We will advise you within one month if we need to extend the response deadline.

Other possible responses:

- We require more information to verify your identity / your legal authority to make a request on another individuals behalf
- we need more information to respond to the request
- we require you to pay a fee before we respond to the request

If we cannot honour the request we will inform you of the reason why, subject to any legal or regulatory restrictions by DD/MM/YYYY.

If you have any questions at this time, on the status of your request please email them to GDPR@ipswich.school.

Yours sincerely

MRR
Compliance Officer

Letter Two - **Request for further information**

Name (Requester)
Address
Date:

Dear XXXXX
Reference: Subject Data Request XX

We write further to our acknowledgement of receipt of your initial request dated DD/MM/YYYY.

Proof of Identity Required.

We require proof of your identity before we can respond to your request. Unfortunately, we cannot verify your identity based on the information given.
To establish your identity please can you provide documentation that clearly shows your Name, DOB and current address. We accept a photocopy or scanned image of the following as proof of identity:

- Passport
- Driving Licence
- Birth or adoption certificate

Please submit your documentation via email and/or by secure mail, so that we can complete your request.

AND/OR
Proof of Identity Required.

We require proof of your legal authority to act on behalf of (DATA SUBJECT). Unfortunately, we cannot verify your legal authority based on the information given. We accept any proof of your legal authority, signed written consent from the data subject, a certified copy of a Power of Attorney, or evidence of parental responsibility if the data subject is a child.

AND/OR
Proof of the data subject's Identity Required.

To help us establish the data subject's identity, you must provide identification that clearly shows the data subjects name, DOB and current address. We accept a photocopy or scanned image of the following as proof of identity:

- Passport
- Driving Licence
- Birth or adoption certificate

If the data subject has changed their name (Marriage) please provide the relevant documents evidencing the change.

AND/OR
Request for Clarification
In order for us to process your request, we require more information about the personal data your request relates to. To help us process and locate the relevant personal data, please provide more information about (Missing Information)

If you have any questions at this time, on the status of your request please email them to GDPR@ipswich.school.
Yours sincerely
MRR

Letter Three - **Response**

Name (Requester)
Address

Date:

Dear XXXXX

Response to Subject Data Request Dated, Reference Number XX

We write in response to the above request dated DD/MM/YYYY.
DPA 18 grants data subjects the right to:

(a) Obtain confirmation that Ipswich School processes their data
(b) Receive certain information about the processing
(c) Receive copies of the data we process

In addition to the access right, DPA 18 also grants data subjects the right to:

(a) Request correction or erasure of their personal data
(b) Restrict or object to certain types of data processing
(c) Make a complaint with the ICO

For further information on the rights granted under DPA 18 please see Ipswich School Privacy notices.

We have received your request and have determined that we are unable to verify your legal authority to make the request on the data subjects behalf and therefore we cannot honour your access request.

Or
After conducting a diligent search for records relating to your access request, we, Ipswich School, have destroyed/erased, or made the personal data anonymous in accordance with our data retention policy.

Or
After conducting a diligent search for records relating to your access request, we, Ipswich School, have confirmed that we process your/data subjects personal data. DPA 18 entitles the data subject to the following:

1. We process the following categories of personal data
2. We process the following categories of personal data for the following purposes
3. etc.

Or
We are unable to process your request as this would violate the rights and freedom of 3rd parties.

If you have any questions at this time, on the status of your request please email them to GDPR@ipswich.school.

Yours sincerely
MRR

Attachment 3 - SAR Log

Subject access request log

No	Name/ Details	Date SAR Received	ID		Reason for SAR	Expire Date (1 Month)	Third Party Data	Complied with (date)
			Requested	Received			Consent Y/N	