Southerly Point Co-operative Multi-Academy Trust
DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

Equality Impact Assessment

The EIA has not identified any potential for discrimination or adverse impact and all opportunities to promote equality have been taken.*	✓
The EIA has not identified any conflict with the Trust's co-operative values and the Church Schools' values.	✓
Adjust the policy to remove barriers identified by the EIA or better promote equality.	✓

*Inclusive of protected characteristics

Provenance	**Date**
Working Party	
HR checks	
Union Consultation	
Staff Consultation	Oct 2020
Trustees' Ratification	Oct 2020
Implementation	Nov 2020

Review Dates
May 2020
October 2020: Changes to names of Trust roles and Trust leadership structures. P18. Mobile devices. Enabling 'hide user ID' facility if necessary to use personal mobile devices to call parents and Covid amendment.
September 2021

To be read in conjunction with:	**Online Safety and Data Security Policy**

Self Help Self Responsibility Equity Equality Democracy Solidarity
Social Responsibility Honesty Openness Caring for Others

Southerly Point Co-operative Multi-Academy Trust

DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

The objective of the policy is to ensure that the school acts within the requirements of the General Data Protection Regulation, which came into force in the UK on 25th May 2018. The policy also seeks to clarify the process by which the school will respond to enquiries for other information is also legal under the Freedom of Information Act 2000 [in force from 1st January 2005].

The member of staff with overall responsibility for personal data within the Trust is the data controller, who is the Trust Executive Leader. Each school has a designated senior leader with delegated responsibility for the implementation of this policy. The Trust also has a Data Protection Officer who is Dave Dudley.

What is Personal Information?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, video or photographic data, location data or online identifier.

General Data Protection Principles

The Trust will comply with Article 5 of the GDPR which requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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;

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 GDPR in order to safeguard the rights and freedoms of individuals; and

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.

The Lawful basis for processing data

In line with the GDPR the Trust and its schools will only process personal data if there is a lawful basis. The Trust or its schools will only process data if there is a contractual right, legal obligation or it enables the Trust or its schools to carry out its Public task. In some situations the Trust or its schools will seek the consent of parents/carers or students over 13.

The school's privacy notice and the impact assessment register will state upon which lawful basis personal data is processed.

The rights of data subjects

The school recognises that data subjects have specific rights under GDPR which are outlined in appendix 1.

The school will issue an annual privacy notice for staff and pupils to enable them to be aware of their rights under GDPR [see appendix 2].

School staff have a right of access to personal data on themselves.

Privacy by Design

In line with the requirements of GDPR, the information asset register, data flow map and privacy impact assessment is reviewed annually by the delegated member of staff for each school. Where any new data process is introduced to the school it must be added to the information asset register, and before it is adopted in the school, the data flow map must be updated and privacy impact assessment must be conducted. If the new process places the data subjects' rights and freedoms at risk, then additional guidance must be sought from the Trusts' data protection officer before the school uses the new data process.

Processing, storing, archiving and deleting personal data

- The school maps the data flow on an annual basis to monitor the processing of personal data for pupils and for staff.
- Each data process has been impact assessed and all reasonable steps have been taken to ensure that the data process is kept secure, and processed only within the remit of the GDPR.
- Personal data and school records about pupils are confidential to the child. This information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. In order to fulfil its public task, GDPR permits such information to be shared with other educational establishments when pupils change schools.
- Educational records for a child will be kept in line with the retention schedules outlined in the IRMS toolkit for schools document, usually until the child reaches 25 years of age, and examination records the same. Paper copies will be stored securely in the school archive once the pupil has left the school, and electronic data, including emails are removed when no longer required.
- Data on staff is will be treated as sensitive information and confidential to the individual, and is shared, only when there is a lawful basis, or at the discretion of the Head Teacher and with the knowledge, and unless an exemption applies, the consent of the staff member concerned.
- Employment records form part of a staff member's personnel file. These records will be retained outlined in the IRMS toolkit for schools document [for six years after the termination of employment]. Paper copies will be stored securely in the school archive once the member of staff has left the school, and electronic data is removed when no longer required.
- Interview records, CV's and application forms for unsuccessful applicants are kept for 6 months.
- All formal complaints made to the Head Teacher or school Governors will be kept for up to 10 years from the date of resolution of the complaint in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.
- A full school retention schedule is available for the full range of personal data and will be checked for compliance before appropriate archiving or disposal of personal data takes place.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen. The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

Data security

- Each data process has been impact assessed and all reasonable steps have been taken to ensure that the data process is kept secure, and processed only within the remit of the GDPR.
- Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- The school restricts staff access to its Management Information System, with a unique username and password. The Server is separated into distinct drives, allowing more sensitive data to be restricted to specific members of staff.
- Staff should not store pupil data on areas of the network which pupils can access.
- Emails should not be used to send personal or sensitive data outside of the school. If there is no other means of responding to a legitimate request for information staff must inform the senior member of staff with responsibility for data security and seek additional guidance. See Appendix 4 for further guidance.
- Staff should avoid the use of USB memory drives to store personal data, and should use remote desktop to process any personal data stored on the school server. If using remote desktop is not a viable option, USB memory drives containing personal information must be encrypted. Further guidance is documented in appendix 3.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared multi-function print, fax, scan and copiers are used. These devices are password protected to minimize risk.
- When not in use, staff should keep any paper based personal data secure, in a form of lockable storage in school and at home.

Accessing personal data: Rights of Access

- A child who is deemed competent can request access to his/her own data. The request is not charged and does not have to be in writing. Senior staff will judge whether the request is in the child's best interests, and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion.
- A parent can request access to or a copy of their child's school records and other information held about their child. The request must be made in writing. There is a charge for such requests on behalf of the child, this is detailed in guidance available from the Information Commissioner. Staff should check, if a request for information is made by a parent, that no other legal obstruction [for example, a court order limiting an individual's exercise of parental responsibility] is in force.
- Parents should note that all rights under GDPR rest with the child. However, the school's legal and public duty allow us to share information with parents regardless of the child's wishes. The following exceptions to this are if the child is in counselling, or has made a medical referral to nurse etc and therefore has a full right to privacy. We cannot share this information without their permission if they are deemed competent.
- For safeguarding matters, if the situation requires that parents need to be informed further advice should be sought from the data protection officer.
- If there is an imminent risk to life or a safeguarding matter you should share sufficient data to prevent the harm occurring. You DO NOT need the consent of the Data Subject to do this.
- There are different mechanisms for dealing with personal and non-personal data. Personal data requests will be dealt with through a subject access request. Requests for non-personal data will be dealt with as a Freedom of Information or Environmental Information Request.
- For further information outing procedures for dealing with requests for information see appendix 6.
- Under the Freedom of Information Act 2000, all schools [primary, secondary and nursery] should have a 'publication scheme' – essentially a formal list of the types of non-personal information which the school produces or holds, and which is readily accessible to staff, pupils and parents or other enquirers. See Appendix 7
- The publication scheme is posted on the school website and can be made available as a hard copy if requested.
- Information which is not covered by the publication scheme can be requested by individuals within or outside the school under the Freedom of Information Act and Environmental Regulations Act.
- If it is a valid FOI request the school will provide guidance on where to access the information required eg. the website link, or details of a charge if the publication/ information is charged, or send any free information. If the item is charged the school does not need to provide it until the payment is received. In these cases the school must give the person requesting the information notice in writing [the "fees notice" Appendix 8] stating that a fee of the amount specified in the notice is to be charged for complying. We reserve the right to refuse to supply information where the cost of doing so exceeds the statutory maximum, currently £450.
- A refusal of any information requested must state the relevant exemption which has been applied or that the school does not hold the information, and must explain what public interest test has made if this applies. FOI requests that would reveal third party personal data may breach the principles of GDPR and therefore require a consideration of whether there would be such a breach in the event of disclosure.
- If the information is published by another organisation [for example, Ofsted reports, DfE leaflets] the school can direct the enquirer to the organisation which supplied the information or publication unless it is legal and possible to provide the information direct [for example, a copy of the summary of an Ofsted report, spare copies of a DfE leaflet].
- It will not be legal to photocopy a publication in its entirety and supply this to an enquirer unless the school owns the copyright – this is particularly important where the original publication was a charged item.
- The school will keep the original request and note against this who dealt with the request and when the information was provided.
- Any complaint about the provision of information will be handled by the Trust's data controller or Trust Executive Leader. All complaints should be in writing and documented. The Publication Scheme will include information on who to contact for both enquiries and complaints.

All enquirers should be advised that they may complain to the Information Commissioner if they are unhappy with the way their request has been handled.

Fair processing of personal data: data which may be shared

Schools, local education authorities and the Department for Education [DfE] all hold information on pupils in order to run the education system, and in doing so will comply with GDPR. The school has carried on an impact assessment for each organisation or individual to whom personal data may be lawfully shared. The school reserves the right to withhold information from a specific third party if there are concerns regarding their compliance with GDPR.

If there is an imminent risk to life or a safeguarding matter, sufficient data should be shared to prevent the harm occurring. The consent of the Data Subject is NOT NEEDED in these circumstances.

Staff should only pass on personal data to external third parties [either software or in person] if they have previously been approved in the impact assessment carried out by the school's SLT, and discussed the request with DPO if there is a high risk to the data subject.

Staff should not sign up to new software which collects personal data without discussing the proposal with the senior member of staff with responsibility for data security and seek additional guidance.

If consent is being used as the lawful basis upon which to share information to a third party, the school should ask what the preferred method of communication is with that third party at the same time of requesting consent.

The school has Fair Processing or Privacy Notices which explain how personal data is used and with whom it will be shared. These are contained in Appendix 2**.** There are separate notices for staff and pupils.

Data breaches

The ICO defines a data breach as 'a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals'.

All schools should approach data breaches with openness and honesty. The member of staff with responsibility for data security should be informed and the school's data protection log updated. All schools should share their anonymised data protection log with the MAT's data protection log annually, to review and adapt working practice.

All data breaches which have the potential to have a significant effect on the data subject will be recorded in the school's data protection log and reported to the Trust's Data Protection Officer immediately. The data protection officer will inform the CEO and the ICO within 72 hours of discovery. The report will contain details of the breach, who was affected the type of data at risk and what the school has done to minimise the impact. If the breach is 'high risk' to the individual affected then the data subject will also be notified.

Persistent breaches or a major breach of data protection policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Pupils who breach this policy will be sanctioned in accordance with the school's behaviour policy.
Article 58 of GDPR sets out the power that the supervisory authority [the ICO] will have to impose corrective obligations on data controllers and processors. Further details are found in appendix 9.

Accountabilities

The Trust's data controller is the Trust Executive Leader, who is responsible for ensuring that any processing of personal data for which they are responsible complies with GDPR.

The Trust's Data Protection Officer is accountable for:

1. Annually reviewing the overall Trust information asset register, data flow map and privacy impact assessment.
2. Conducting an annual inspection of the schools to ensure that they are compliant with the Trust policy.
3. To maintain a Trust-wide log of data protection breaches.
4. To summarise the causes and emerging actions of any data protection breaches.
5. To co-ordinate all FOI and SAR which are received by any schools within the Trust.
6. To be the first point of contact for supervisory authorities and for individuals whose data is processed [employees, customers etc].

7. To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

Each school should have a named senior leader with responsibility for data protection. They are accountable for:

1. Maintaining the information asset register, data flow map and privacy impact assessment for their school.
2. Conducting an annual inspection of the school to ensure that they are compliant with the Trust policy.
3. Providing a report to the Trust DPO with areas of compliance and further actions required.
4. To maintain a school-wide log of data protection breaches, and forward information relating to breaches to the DPO.
5. To summarise the causes and emerging actions of any data protection breaches.
6. To inform the DPO and Trust Executive Leader of any FOI or SAR that the school receives.

Each data process or asset has an owner. This is documented in the information asset register. Each data owner is accountable for:

1. Ensuring that the actions noted in the privacy impact asset are carried out so that data is processed securely and in line with the lawful basis.
2. Taking all reasonable steps to ensure that any information passed onto third parties is done so in accordance with GDPR requirements.
3. Taking all reasonable steps to ensure that the data process or asset is monitored to ensure that data breaches are kept to a minimum.
4. To log and report any data breaches to the school's designated senior leader.

All members of staff are data processors. Their behaviour must also comply with the regulations outlined by GDPR. For example all staff should:

1. Treat all personal data that they encounter regarding either staff or pupils as confidential.
2. Keep data secure when not in used and avoid taking it off the school site. If this is unavoidable steps must be taken to protect the security of the data.
3. Be aware that privately owned ICT equipment should not be used on the school network, but access the internet through the school Wi-Fi is allowed at the discretion of the designated Senior Leader. Staff should not use their own ICT equipment [this includes, USB memory devices or portable hard drives] in the school, and the school doesn't acceptable any liability if staff do bring their own ICT equipment into school.
4. As far as is reasonably possible, avoid storing personal or sensitive data on the local drives of desktop PCs, laptops, USB memory sticks or other portable devices. If it is necessary to do so the local drive must be encrypted.
5. Staff must be familiar with the AUA and act in line with its requirements.
6. Only use the school's information management system [eg SIMS], or network, solely for the completion of specific duties for their designated role in the school.
7. Take care not to accidently share personal information with other individual, for example through digital projectors in the classroom.
8. Inform the School's senior member of staff if you would like to start a new data process [e.g. use a new piece of software]

Appendices

Appendix 1 – The rights of data subjects under GDPR

Appendix 2 - Draft Privacy Notice for Pupils and Staff

Appendix 3 – Summary Guidance for Volunteers and Supply Staff

Appendix 4 – Using Portable & Mobile ICT Equipment & Removable Media
Appendix 5 – Additional guidance regarding emails
Appendix 6 – Dealing with requests for information - Process Map
Appendix 7 – Freedom of Information Publication Scheme
Appendix 8 – Freedom of Information Fees Notice
Appendix 9 – Details of corrective action the ICO can impose on the Trust
Appendix 10 – Glossary of terminology

Appendix 1 - The Rights of Data Subjects under GDPR

(a) The right to be informed – The school will provide children with the same information about how the school processes their personal data as with adults. Information will be concise clear and presented in an age appropriate manner.

(b) The right of access - Under GDPR, pupils are data subjects and can access to their own personal information if they are deemed competent. Those with Parental Responsibility can only access the personal information of their child if their child has given specific consent or is deemed not competent. Currently parents do not have a legal right to access their child's educational record in Academies and Free schools.

(c) The right to rectification - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

(d) The right to erasure – Individuals have the right to request that personal data is removed for specific reasons, however, exemptions to this right apply and the school will consider these exemptions when responding to the request. The school will not keep personal information for longer than is required and will use the IRMS Information Toolkit for schools for retention schedules.

(e) The right to restrict processing – Individuals have the right to request that their personal data is no longer processed but simply stored. Exemptions to this right apply and the school will consider each request on a case by case basis.

(f) The right to data portability – Individuals have the right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. The school will provide the personal data in a structured, commonly used and machine readable form.

(g) The right to object - Individuals can object to the processing of their personal data on "grounds relating to his or her particular situation". The school will stop processing the personal data unless:

a. There are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
b. The processing is for the establishment, exercise or defence of legal claims.

(h) Rights in relation to automated decision making and profiling – The school does not engage in any automated decision making or profiling.

Appendix 2 – Draft Privacy Notice for Pupils and Staff

FAIR PROCESSING [PRIVACY] NOTICE

PUPILS

Mullion Primary School

This policy is to let you know how **Mullion Primary School** will collect, use and process personal data. It is also designed to let you know your rights and what you can do if you have questions about personal data.

The School is the controller for the purposes of data protection laws.

This document sets out the types of personal data [meaning information about an individual from which that individual can be personally identified] we handle, the purposes of handling those personal data and any recipients of it.

Our details

We are: **Mullion Primary School**

Registered Company Number: 10552443 [for Southerly Point Co-operative Multi-Academy Trust]

Address: Willis Vean Muullion TR12 7DF

Information Commissioner's Office Registration Number: ZA258622 [for Southerly Point Co-operative Multi-Academy Trust]

Our Data Protection Officer is: Dave Dudley

and their contact details are: Helston Community College, Church Hill, Helston, Cornwall

Why we collect data

We collect and hold personal information relating to our pupils and may also receive information about them from their previous schools, the Local Authority, Department for Education [DfE] and other bodies linked to their education, development and welfare. We may also share personal data with other agencies as necessary under our legal duties or otherwise in accordance with our duties/obligations as a school.

Whilst the majority of pupil information we are provided with or collect is mandatory, some of it is provided to us on a voluntary basis. We will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Below are set out the reasons why we collect and process personal data, as well as the legal basis on which we carry out this processing:

- **To support our pupils' learning**: we will process personal data to help every child achieve his or her potential in all areas of learning and to promote excellence in our teaching and learning environment.
- **Monitor and report on their progress**: we will process personal data to record pupils' progress to help set and monitor targets and boost achievements and aspirations of all pupils.
- **Provide appropriate pastoral care**: we will process personal data to ensure that all pupils are properly supported in their time with us. We will process data to help staff understand and respond to the unique circumstances of all pupils.
- **Assess the quality of our services**: we will process personal data so that we may reflect on our own practices to help us improve and provide the highest quality education that we can to all pupils.
- **To ensure proper management of school trips and afterschool clubs and activities**: when pupils and parents participate in school trips and afterschool clubs and activities personal data will need to be processed.
- **To promote and protect health and safety**: in order to protect pupils, parents and staff in their involvement at the school, we must process personal data relating to matters such as incidents and responses to incidents.

Legal Basis for Processing

The lawful basis for us to collect/process this personal data is in order to provide education in accordance with statute law [such as the Education Act 1996 and other legislation], our funding agreements with the Secretary of State, our memorandum and articles of association and other guidance provided for in law.

In addition, personal data will be collected and/or processed for the purposes of relevant contracts for the provision of services which are paid for. This may include but is not limited to:

- The provision of music tuition;

- School trips;
- Entering pupils for examinations.

We do not process any special categories of personal data except where necessary for reasons of substantial public interest in complying with legal obligations including under the Equality Act 2010 or where necessary to protect the vital interests of the data subject or of another natural person and where safeguards are in place to ensure that this personal data is kept secure. For the avoidance of doubt where special categories of personal data are collected it shall not be used for the purposes of automated decision making and/or profiling.

Special categories of data means personal data revealing:

- *racial or ethnic origin;*
- *political opinions; religious or philosophical beliefs or trade union membership;*
- *genetic or biometric data that uniquely identifies you;*
- *data concerning your health, sex life or sexual orientation; or*
- *data relating to criminal convictions or offences or related security measures.*
- *Further personal data including special categories of personal data may be collected and/or processed where consent has been given [for example, school photographs for non-educational purposes]. If consent has been given then this may be revoked in which case the personal data will no longer collected/processed.*

For photographs and or videos we will seek consent from pupils over 13 or their parents for younger pupils, on an annual basis. This will allow pupils and parents the right to give consent for the manner in which this form of personal data is processed and shared.

Categories of information we collect

We may collect the following types of personal data [please note this list does not include every type of personal data and may be updated from time to time]:

- contact details;
- data of birth;
- health and/or other medical information;
- information in connection with education [included but not limited to unique pupil numbers, test results, post 16 learning information and other records];
- attendance information;
- behavioural and disciplinary information;
- free school meal eligibility;
- information received in connection with any complaint;
- personal characteristics of pupils, such as:
    - their nationality and ethnic group;
    - their religion;
    - their first-language;
    - any special educational needs they may have;
    - any relevant protected characteristics.

Who will have access to your data

Personal data will be accessible by members of staff. Where necessary, volunteers and governors will also have access to personal data.

We will not share information about our pupils with third parties without consent unless we are required to do so by law or our policies. We will take all steps reasonably necessary to ensure that once your personal data is shared it is treated securely and in accordance with this privacy policy. We will disclose personal data to third parties:

- if we are under a duty to disclose or share your personal data in order to comply with any legal obligation; for example, we share pupils' personal data with the Department for Education on a statutory basis;
- in order to enforce any agreements with you;
- to protect the rights, property, or safety of the School, the school, other pupils or others. This includes exchanging information with other organisations for the purposes of child welfare.

This may include our Local Authority, the Department for Education, the Police and other organisations where necessary; for example, for the purposes of organising a school trip or otherwise enabling pupils to access services or for the purposes of examination entry. Information may also be sent to other schools where necessary; for example, schools that pupils attend after leaving us.

How data will be processed

Personal data may be processed in a variety of ways; this will include but is not limited to:

- sending by e-mail;
- adding to spreadsheets, word documents or similar for the purposes of assessing personal data;
- for educational software use [this could be for the purposes of helping children learn, discipline, reports and other educational purposes].

Where we store data and how we keep data secure

Paper copies of personal data are kept securely at the school; for example, in secure filing cabinets.

Electronic copies of personal data are kept securely and information will only be processed where we are satisfied that it is reasonably secure.

All information you provide to us is stored on secure servers. Where we have given you [or where you have chosen] a password which enables you to access certain parts of our website, you are responsible for keeping this password confidential. You must not share your password with anyone.

When giving personal data to third parties [for example, software providers] it is possible that this personal data could be stored in a location outside of the European Economic Area. We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this privacy policy. In particular, any transfer of your personal data made by us to a location outside of the EEA will be governed by clauses in a written contract in order to keep these secure.

Retention periods

We will only retain personal data for as long as is necessary to achieve the purposes for which they were originally collected. As a general rule, personal data will be kept for the entire period that a child is a pupil at the school. Other records [for example, safeguarding or in relation to special educational needs] will be kept for longer in accordance with guidance from the Local Authority. Further information on retention periods can be obtained by contacting us via the details in this Notice.

Your data rights

The General Data Protection Regulation and associated law gives you rights in relation to personal data held about you and your child. These are:

- **Right of Access**: if your personal data is held by the School, you are entitled to access your personal data [unless an exception applies] by submitting a written request. We will aim respond to that request within one month. If responding to your request will take longer than a month, or we consider that an exception applies, then we will let you know. You are entitled to access the personal data described in this privacy notice.
- **Right of Rectification**: you have the right to require us to rectify any inaccurate personal data we hold about you. You also have the right to have incomplete personal data we hold about you completed. If you have any concerns about the accuracy of personal data that we hold then please contact us.
- **Right to Restriction**: you have the right to restrict the manner in which we can process personal data where:
    - the accuracy of the personal data is being contested by you;
    - the processing of your personal data is unlawful, but you do not want the relevant personal data to be erased; or

- we no longer need to process your personal data for the agreed purposes, but you want to preserve your personal data for the establishment, exercise or defence of legal claims.

Where any exercise by you of your right to restriction determines that our processing of particular personal data are to be restricted, we will then only process the relevant personal data in accordance with your consent and, in addition, for storage purposes and for the purpose of legal claims.

- **Right to Erasure**: You have the right to require we erase your personal data which we are processing where one of the following grounds applies:
    - the processing is no longer necessary in relation to the purposes for which your personal data were collected or otherwise processed;
    - our processing of your personal data is based on your consent, you have subsequently withdrawn that consent and there is no other legal ground we can use to process your personal data;
    - the personal data have been unlawfully processed; and
    - the erasure is required for compliance with a law to which we are subject.
- **Right to Data Portability**: you have the right to receive your personal data in a format that can be transferred. We will normally supply personal data in the form of e-mails or other mainstream software files. If you want to receive your personal data which you have provided to us in a structured, commonly used and machine-readable format, please contact us via the details in Section 1 of this Notice.

You can find out more about the way these rights work from the website of the Information Commissioner's Office [ICO].

Requesting your data

Where the School holds personal data concerning you, you are entitled to access that personal data and the following information [unless an exception applies]:

- a copy of the personal data we hold concerning you, provided by the School;
- details of why we hold that personal data;
- details of the categories of that personal data;
- details of the envisaged period for which that personal data will be stored, if possible;
- information as to the source of personal data where that personal data was not collected from you personally.

If you want to receive a copy of the information about your son/daughter that we hold, please contact us via the details at the start of this Notice.

Making a Complaint

If you are unhappy with the way we have dealt with any of your concerns, you can make a complaint to the ICO, the supervisory authority for data protection issues in England and Wales. We would recommend that you complain to us in the first instance, but if you wish to contact the ICO on the details you can do so on the details below. The ICO is a wholly independent regulator established in order to enforce data protection law.

ICO Concerns website: www.ico.org.uk/concerns

ICO Helpline: 0303 123 1113

ICO Email: casework@ico.org.uk

ICO Postal Address: *Information Commissioner's Office*
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Changes to this notice

Any changes we make to this notice in the future will be posted on our website and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes.

FAIR PROCESSING [PRIVACY] NOTICE

WORKFORCE

Mullion Primary School

This policy is to let you know how **Mullion Primary School** will collect, use and process personal data. It is also designed to let you know your rights and what you can do if you have questions about personal data.

The School is the controller for the purposes of data protection laws.

This document sets out the types of personal data [meaning information about an individual from which that individual can be personally identified] we handle, the purposes of handling those personal data and any recipients of it.

Our details

We are: **Mullion Primary School**

Registered Company Number: 10552443 [for Southerly Point Co-operative Multi-Academy Trust]

Address: Church Hill, Helston

Information Commissioner's Office Registration Number: ZA258622 [for Southerly Point Co-operative Multi-Academy Trust]

Our Data Protection Officer is: Dave Dudley

and their contact details are: Helston Community College, Church Hill, Helston, Cornwall

Why we collect data

We collect and hold personal information relating to the school workforce and may also receive information about them from previous employers, the Local Authority, Department for Education [DfE] and other professional bodies. We may also share personal data with other agencies as necessary under our legal duties or otherwise in accordance with our duties/obligations as a school.

Whilst the majority of workforce information we are provided with or collect is mandatory, some of it is provided to us on a voluntary basis. We will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Below are set out the reasons why we collect and process personal data, as well as the legal basis on which we carry out this processing:

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid

Legal Basis for Processing

The lawful basis for us to collect/process this personal data is in order to provide education in accordance with statute law [such as the Education Act 1996 and other legislation], our funding agreements with the Secretary of State, our memorandum and articles of association and other guidance provided for in law.

In addition, personal data will be collected and/or processed for the purposes of relevant contracts for the provision of services which are paid for.

We do not process any special categories of personal data except where necessary for reasons of substantial public interest in complying with legal obligations including under the Equality Act 2010 or where necessary to protect the vital interests of the data subject or of another natural person and where safeguards are in place to ensure that this personal data is kept secure. For the avoidance of doubt where special categories of personal data are collected it shall not be used for the purposes of automated decision making and/or profiling.

Special categories of data means personal data revealing:

- *racial or ethnic origin;*

- *political opinions; religious or philosophical beliefs or trade union membership;*
- *genetic or biometric data that uniquely identifies you;*
- *data concerning your health, sex life or sexual orientation; or*
- *data relating to criminal convictions or offences or related security measures.*
- Further personal data including special categories of personal data may be collected and/or processed where consent has been given [for example, school photographs for non-educational purposes]. If consent has been given then this may be revoked in which case the personal data will no longer Categories of information we collect

We may collect the following types of personal data [please note this list does not include every type of personal data and may be updated from time to time]:

- contact details;
- data of birth;
- health and/or other medical information [including confirmation of fit to work];
- information in connection with education [including academic and other qualifications];
- attendance information;
- behavioural and disciplinary information;
- information received in connection with any complaint;
- biometric data specifically for use with the cashless catering system;
- information required for employment purposes, such as:
    - national Insurance numbers;
    - bank details;
    - remuneration details;

Who will have access to your data

Personal data will be accessible only by specific members of staff, in order to fulfil their contractual role. Where necessary governors will also have access to personal data.

We will not share information about our workforce with third parties without consent unless we are required to do so by law or our policies. We will take all steps reasonably necessary to ensure that once your personal data is shared it is treated securely and in accordance with this privacy policy. We will disclose personal data to third parties:

- if we are under a duty to disclose or share your personal data in order to comply with any legal or contractual obligation; for example, we share bank details with County Payroll, and Appraisal documentation is held by Angel Perspective;
- in order to enforce any agreements with you;
- to protect the rights, property, or safety of the School, or other pupils. This includes exchanging information with other organisations for the purposes of child welfare.

This may include our Local Authority, the Department for Education, the Police and other organisations where necessary.

How data will be processed

Personal data may be processed in a variety of ways; this will include but is not limited to:

- sending by e-mail;
- adding to spreadsheets, word documents or similar for the purposes of assessing personal data;
- for educational software use [this could be for the purposes of helping children learn, discipline, reports and other educational purposes].

Where we store data and how we keep data secure

Paper copies of personal data are kept securely at the school; for example, in secure filing cabinets.

Electronic copies of personal data are kept securely and information will only be processed where we are satisfied that it is reasonably secure.

All information you provide to us is stored on secure servers. Where we have given you [or where you have chosen] a password which enables you to access certain parts of our website, you are responsible for keeping this password confidential. You must not share your password with anyone.

When giving personal data to third parties [for example, software providers] it is possible that this personal data could be stored in a location outside of the European Economic Area. We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this privacy policy. In particular, any transfer of your personal data made by us to a location outside of the EEA will be governed by clauses in a written contract in order to keep these secure.

Retention periods

We will only retain personal data for as long as is necessary to achieve the purposes for which they were originally collected. As a general rule, personal data will be kept for the entire period that a member of staff is employed at the school, and for six years following the termination of their contract. Other records [for example, safeguarding or in relation to special educational needs] will be kept for longer in accordance with guidance from the Local Authority. Further information on retention periods can be obtained by contacting us via the details in this Notice.

Your data rights

The General Data Protection Regulation and associated law gives you rights in relation to personal data held about you. These are:

- **Right of Access**: if your personal data is held by the School, you are entitled to access your personal data [unless an exception applies] by submitting a written request. We will aim respond to that request within one month. If responding to your request will take longer than a month, or we consider that an exception applies, then we will let you know. You are entitled to access the personal data described in this privacy notice.
- **Right of Rectification**: you have the right to require us to rectify any inaccurate personal data we hold about you. You also have the right to have incomplete personal data we hold about you completed. If you have any concerns about the accuracy of personal data that we hold then please contact us.
- **Right to Restriction**: you have the right to restrict the manner in which we can process personal data where:
    - the accuracy of the personal data is being contested by you;
    - the processing of your personal data is unlawful, but you do not want the relevant personal data to be erased; or
    - we no longer need to process your personal data for the agreed purposes, but you want to preserve your personal data for the establishment, exercise or defence of legal claims.

Where any exercise by you of your right to restriction determines that our processing of particular personal data are to be restricted, we will then only process the relevant personal data in accordance with your consent and, in addition, for storage purposes and for the purpose of legal claims.

- **Right to Erasure**: You have the right to require we erase your personal data which we are processing where one of the following grounds applies:
    - the processing is no longer necessary in relation to the purposes for which your personal data were collected or otherwise processed;
    - our processing of your personal data is based on your consent, you have subsequently withdrawn that consent and there is no other legal ground we can use to process your personal data;
    - the personal data have been unlawfully processed; and
    - the erasure is required for compliance with a law to which we are subject.
- **Right to Data Portability**: you have the right to receive your personal data in a format that can be transferred. We will normally supply personal data in the form of e-mails or other mainstream software files. If you want to receive your personal data which you have provided to us in a structured, commonly used and machine-readable format, please contact us via the details in Section 1 of this Notice.

You can find out more about the way these rights work from the website of the Information Commissioner's Office [ICO].

Requesting your data

Where the School holds personal data concerning you, you are entitled to access that personal data and the following information [unless an exception applies]:

- a copy of the personal data we hold concerning you, provided by the School;
- details of why we hold that personal data;
- details of the categories of that personal data;
- details of the envisaged period for which that personal data will be stored, if possible;
- information as to the source of personal data where that personal data was not collected from you personally.

If you want to receive a copy of the information about your son/daughter that we hold, please contact us via the details in Section 0 of this Notice.

Making a Complaint

If you are unhappy with the way we have dealt with any of your concerns, you can make a complaint to the ICO, the supervisory authority for data protection issues in England and Wales. We would recommend that you complain to us in the first instance, but if you wish to contact the ICO on the details you can do so on the details below. The ICO is a wholly independent regulator established in order to enforce data protection law.

ICO Concerns website: www.ico.org.uk/concerns

ICO Helpline: 0303 123 1113

ICO Email: casework@ico.org.uk

ICO Postal Address: Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Changes to this notice

Any changes we make to this notice in the future will be posted on our website and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes.

Appendix 3 – Summary Guidance for Supply and Volunteer Staff

Staff, visitors, governors and volunteers should be familiar with, and work in accordance with, the policies and guidance at **Mullion Primary School** including in particular data protection and online security.

Visitors should treat all personal data that they encounter regarding either staff or pupils as confidential.

Any data which is provided to them as part of their role should remain secure when not in used and not taken off the school site.

Privately owned ICT equipment should not be used on the school network, but access the internet through the school Wi-Fi is allowed at the discretion of the designated Senior Leader. Staff should not use their own ICT equipment [this includes, USB memory devices or portable hard drives] in the school, and the school doesn't acceptable any liability if staff do bring their own ICT equipment into school

Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted.

Visitors must take care not to accidently share personal information with other individual, for example through digital projectors in the classroom.

Some visitors will have access to the school's management information system, and this should be used solely for the completion of the specific duties for which the visitors has to fulfil.

Visitors may also be given a temporary access to the schools LAN or WIFI network. Visitors must be familiar with the Acceptable Use Agreement [AUA] and act in line with its requirements.

Appendix 4 – Using Portable & Mobile ICT Equipment & Removable Media

Portable & Mobile ICT Equipment

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Privately owned ICT equipment should not be used on the school network, but access the internet through the school Wi-Fi is allowed at the discretion of the Headteacher. Staff should not use their own ICT equipment [this includes, USB memory devices or portable hard drives] in the school, and the school doesn't acceptable any liability if staff do bring their own ICT equipment into school
- It is responsibility of the staff member to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- Staff must ensure that all school data is stored on the school network, and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and

software installations, patches or upgrades The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

Mobile telephones

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Under no circumstances does the school allow a member of staff to contact a pupil using their personal device. Members of staff should not use their personal mobile devices to contact parents unless the hide user id facility is enabled. Staff should not contact pupils on the pupil's mobile phones (except in an emergency on a trip / visit; or for Post 16 students)
- Covid Amendment: during lockdown where staff are working remotely they should use a school mobile or where possible the school's 3CX app which shows the school number as caller id. if neither of these options is available , staff may use their personal mobile so long as the hide user id facility is enabled.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- Staff who wish to set up and use a school e-mail account on their personal mobile device will need to have some form of device locking e.g. password or pin. If the device gets lost or stolen, the Network Manager needs to be informed as soon as possible so that the device can be remotely wiped of data.

Appendix 5 - Additional Guidance Regarding Emails

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of a school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsibly online.

Managing e-mail

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the network manager and will automatically be added as a footer. This disclaimer must not be edited or deleted by the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Do not use the e-mail application as a data and file storage system
    - E-mails that need to be kept should be identified for content and filed appropriately [appended to the pupil's communication log in SIMS]
    - Organise e-mail into folders and carry out frequent house-keeping on all folders, retaining emails for a maximum of 18 months
- Staff must inform [the Online Safety Co-ordinator or line manager] if they receive an offensive e-mail
- However, you access your school e-mail, [whether directly, through webmail when away from the office or on personal hardware] all the school e-mail policies apply
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Pupils are introduced to e-mail as part of their curriculum

Sending e-mails

- Staff should use their own school e-mail account so that you are clearly identified as the originator of a message. Having a clearly defined subject line helps the recipient to sort the email on receipt. A clear subject line also assists in filing all emails relating to individual projects in one place.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain emails. If you send a message externally to more than one person, you must hide the recipients' email addresses. You can do this by putting just your own name in the "To" field, and putting the other addresses in the "Bcc" field.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal matters, including personal business, disputes or legal affairs, nor state views that may be libelous or detrimental to the reputation of the school
- Whenever possible, omit personal identifiable data such as names, date of birth, address etc. from any emails. When referring to pupils in emails use their initials in the 'subject' of the email and not their full name.
- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section: e-mailing Personal, Sensitive, Confidential or Classified Information

Receiving e-mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the e-mail systems to store attachments. Where the main purpose of the email is to transfer documents, then the documents should be saved into the appropriate places in an electronic filing system or printed out and added to a paper file. The email can then be deleted.
- When receiving an email containing personal identifiable information about a pupil, parent/carer or member of staff, the email is classified as a record which must be dealt with appropriately under data protection guidelines. In these cases, print off a hard copy and place in the appropriate pupil or staff file and retain in line with the records retention schedule.

- The automatic forwarding of e-mails is not allowed. Do not set up rules to automatically forward your school e-mail to a personal e-mail account for example.

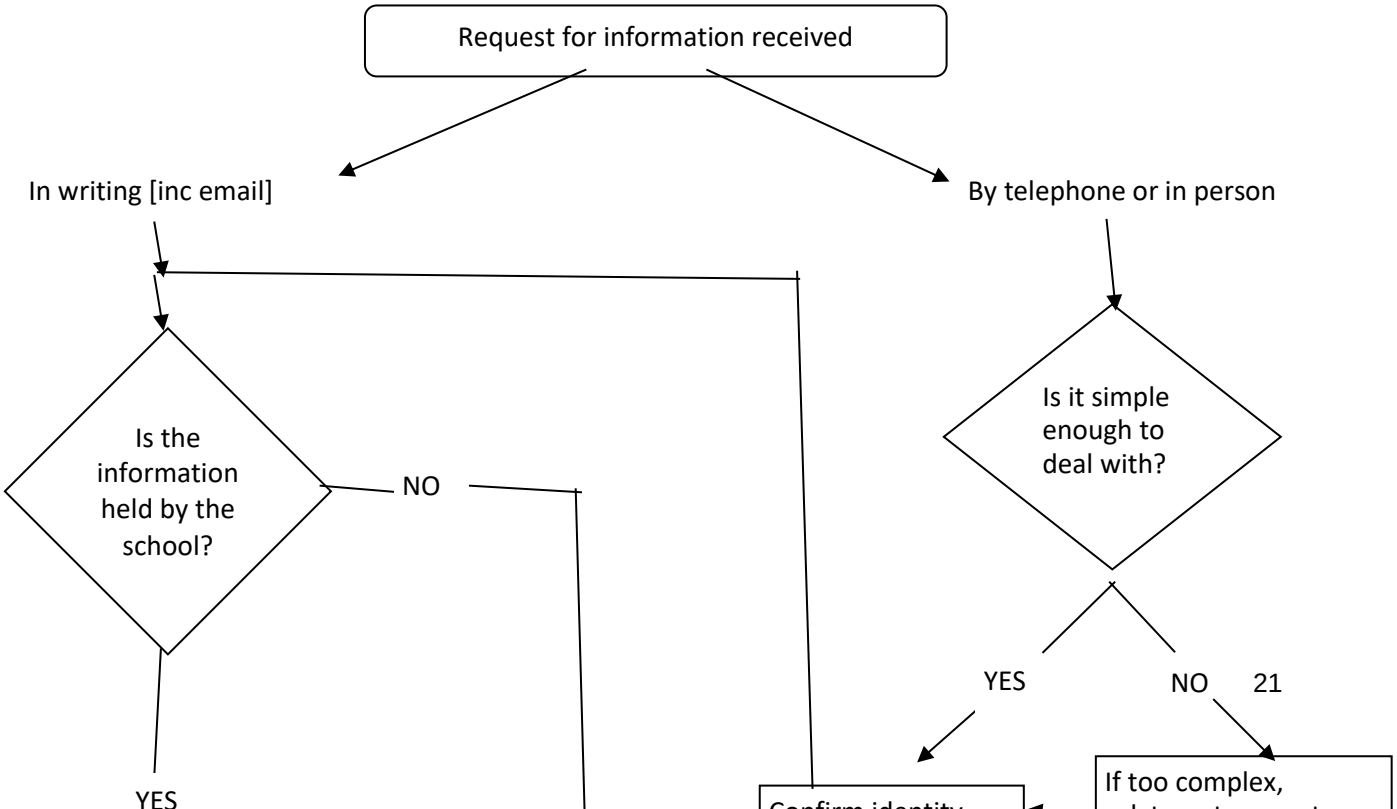
E-mailing Personal, Sensitive, Confidential or Classified Information
Email should only be used to transmit such data if no alternative method is available [eg Egress, Anycoms or Collect]

Obtain express consent from your line manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

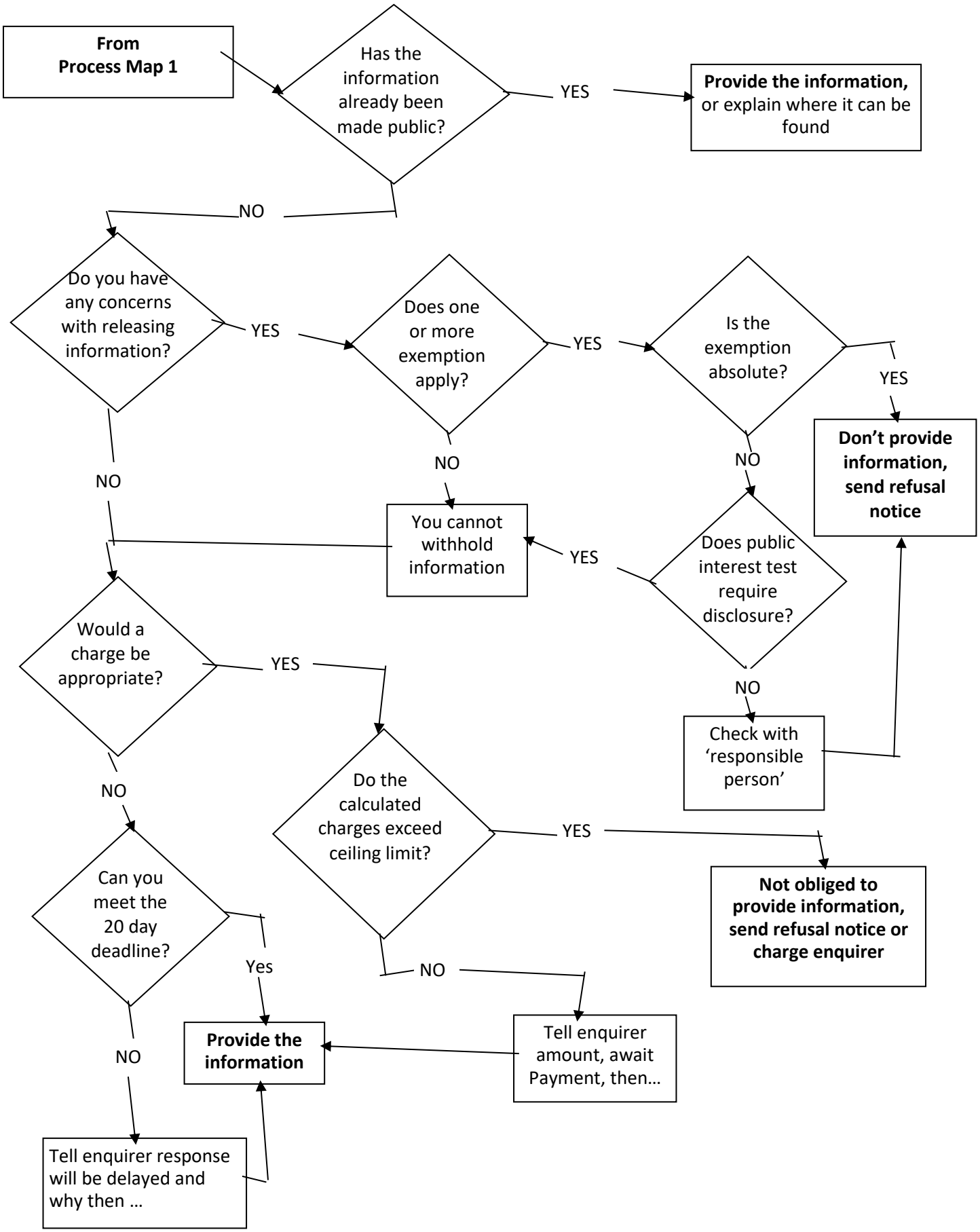
- Encrypt and password protect. See the Network Manager on how to do this.
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify [by phoning] the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify [usually by phone]
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient[s]
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

<u>Appendix 6 – Responding to Requests for Information</u>

PROCESS MAP TO DETERMINE METHOD OF RESPONSE



PROCESS MAP FOR HANDLING FOI ENQUIRIES



Further guidance referring to the procedures for dealing with access request [SARs]

- The request must be made in writing and often the following phrase is used, “a copy of all information held on XXX, including notes, emails, records of conversations, assessments, reports, communications, notes sent and received and all plans”. This phrase requests information contained in the pupil’s Education Record [assessments, reports, and all information in their file]. The other information requested [emails, notes, records of conversations, communications and plans not filed], does not form part of the Educational Record should be dealt with as a SAR.
- For educational records ie: records in the school’s information management system, and in pupil’s paper file [unlike other personal data; see below] access will be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment. The ICO outlines the following charges: For an educational record, it depends on the number of pages provided. For example, 1 to 19 pages will cost £1.20; 29 pages will cost £2, and so on, up to a maximum of 500+ pages which will cost £50.
- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. The school can charge a ‘reasonable fee’ for additional copies of records.
- Under GDPR, pupils are data subjects and can access to their own personal information if they are deemed competent. Those with Parental Responsibility can only access the personal information of their child if their child has given specific consent or is deemed not competent.
- GDPR requires that all requests for personal information are dealt with within one calendar month of receipt except requests for educational records [see above]. All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If awaiting third party consents, the school will arrange access to those documents already available, and notify the individual that other documents may be made available later. The school can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
- In all cases, should third party information [information about another individual] be included in the information the staff will try to obtain permission to show this information to the applicant, with the exception of information provided by another member of school staff [or local authority staff] which is exempt from a requirement for third party consents. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.
- Where information originated from a third party it is advised that the third party is made aware of the SAR, but they cannot prevent its release unless one of the SAR exemptions applied [see SAR exemptions on the ICO website].
- Personal data should always be of direct relevance to the person requesting the information. A document discussing more general concerns may not be defined as personal data.
- From 1st January 2005, when the Freedom of Information Act came fully into force, a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual’s personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work. These can be requested if sufficient information is provided to identify them.
- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes [letter requesting changes etc.] This will enable staff to deal with a complaint if one is made in relation to the request.

Further guidance referring to the procedures for dealing with a Freedom of Information Request [FOI]

Under the Freedom of Information Act [2005] Act, all schools which receive a **written or emailed** request for information which they hold or publish are required to respond within 20 school days [or 60 working days, whichever is shorter].

- Upon receipt of any request the MAT data controller and CEO must be informed without delay.
- When handling a request for information a designated member of the MAT central team will use the process maps contained in this appendix. See also **Appendix 7,** the Freedom of Information Publication Scheme

Appendix 7 – Freedom of Information Publication Scheme

This publication scheme commits Southerly Point Co-operative Multi-Academy Trust to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by Southerly Point Co-operative Multi-Academy Trust.

The scheme commits Southerly Point Co-operative Multi-Academy Trust:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by Southerly Point Co-operative Multi-Academy Trust and falls within the classifications below.
- To specify the information which is held by Southerly Point Co-operative Multi-Academy Trust and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information Southerly Point Co-operative Multi-Academy Trust makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.

2. Classes of information

2.1 Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

2.2 What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

2.3 What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

2.4 Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

2.5 The services we offer.
Information about the services the Trust provides including leaflets, guidance and newsletters.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

3. The method by which information published under this scheme will be made available

Where it is within the capability of Southerly Point Co-operative Multi-Academy Trust, information will be provided on our website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, we will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

4. Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the Trust for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment is required prior to provision of the information.

5. Written requests

Information held by the Trust that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

6. Contact details

If you require a paper version of any information, or want to ask whether information is available please contact the Trust by telephone, email or letter. Contact details are set out below or you can visit our website at

Email: Ddudley@helston.cornwall.sch.uk

Tel: 01326 572022

Contact Address: Helston Community College, Church Hill, Helston TR13 8NR

To help us process your request quickly, please clearly mark any correspondence **"PUBLICATION SCHEME REQUEST**" [in CAPITALS please]. If the information you're looking for isn't available via the scheme and isn't on our website**,** you can still contact the Trust to ask if we have it.

Appendix 8 – Freedom of Information Fees Notice

STATEMENT

This Fees Notice is submitted by **Southerly Point Multi-Academy Trust** in accordance with Section 9 of the Freedom of Information Act 2000 [the FOI Act] and requires the payment of the fee[s] within a period of three months, beginning with the day this Fees Notice is received by the Applicant. Failure to pay the fee[s] within the prescribed period will result in the discharge of Southerly Point Multi-Academy Trust's obligations under the FOI Act.

Please read the Note accompanying this Fees Notice

1. Applicant's Details

NAME:

ADDRESS:

TEL:

FAX:

EMAIL:

2. Information Requested

3. Applicant's request applies to documents from **to**

4. Fees Due **£**

1. search, retrieval and collation
2. photocopying
3. printing
4. postage
5. priced publication
6. any other disbursements

Total Due **£**

Date:

Please make your payment by cheque, payable to Southerly Point Multi-Academy Trust and forward your cheque to: Mr D. Dudley

Whilst Southerly Point Multi-Academy Trust must respond to your request for information within 20 working days of the date of receipt of your application, please note that this time period does not begin to run until you have paid the fee[s].

If you pay the fee[s] within a period of three months, the Southerly Point Multi-Academy Trust must, subject to the consideration of exemptions, comply with your request for the information detailed in your application and this Fees Notice.

NOTE

Fees are regulated by Fees Regulations and the 'appropriate fee' for Southerly Point Multi-Academy Trust as a public authority is £450.00 [referred to in this Note as the 'Threshold']. Where charges apply, a Fees Notice will be sent to you within 20 working days' of receipt of your written application. You must pay the specified fee within 3 months of receiving the Fees Notice. If payment is not made within this period, Southerly Point Multi-Academy Trust is not obliged to process your application; in other words the clock stops while Southerly Point Multi-Academy Trust is awaiting payment from you.

NB: The period beginning with the giving of the Fees Notice and ending with receipt of the fee by Southerly Point Multi-Academy Trust is disregarded in calculating the period required for Southerly Point Multi-Academy Trust to comply with the request for information.

Search, retrieval and collation

Where the information you are seeking is already available in a priced publication, Southerly Point Multi-Academy Trust will provide you with details of the publication and where to obtain it.

Southerly Point Multi-Academy Trust is not obliged to comply with your request for information if Southerly Point Multi-Academy Trust estimates that the search, retrieval and collation costs of complying with the request would exceed the Threshold. The School will however give an indication of the information which could be provided within/below the Threshold.

Estimated costs below the Threshold:

There will be no charge for the search, retrieval and collation etc of information where the costs are estimated to be less than the Threshold. Southerly Point Multi-Academy Trust may, however, charge the full costs of disbursements e.g. photocopying, postage, video, tape, disk, computer runs etc.

Estimated costs above the Threshold:

Should the time for complying with your request be estimated to exceed 18 hours, there will be a charge of £450 based on £25 per hour per person. In addition to the hourly rate, the School may charge the full costs of disbursements e.g. photocopying, postage, video, tape, disk, computer runs etc. Please note that Southerly Point Multi-Academy Trust is not required to comply with the request should it exceed the Threshold.

Multiple requests:

Where two or more requests are made by the same person, or by different persons who appear to be acting in concert, or in pursuance of a campaign, Southerly Point Multi-Academy Trust will regard theses as one request and estimated costs will be calculated accordingly. This will apply for a period of sixty consecutive working days from the first request.

If your request falls within this category, you will be provided with an estimate of the cost of providing the information before the Southerly Point Multi-Academy Trust starts any work on your behalf.

Appendix 9– details of corrective action that the ICO can impose.

Article 58 of GDPR sets out the power that the supervisory authority [the ICO] will have to impose corrective obligations on data controllers and processors:

- warnings that organisations are likely to infringe the GDPR
- reprimands where there has been an infringement
- order to comply with the request of a data subject
- order to communicate a personal data breach to a data subject
- impose a limitation including a ban on processing
- order to rectify, restrict or erase data
- withdraw certification
- suspend the flow of data to a third country or international organisation
- impose an administrative fine

Administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive".

There are two tiers of administrative fines that can be levied:

1] Up to €10 million, or 2% annual global turnover – whichever is higher.
2] Up to €20 million, or 4% annual global turnover – whichever is higher.

Appendix 10 – Glossary of Terminology

Acceptable Use Agreement - a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

Biometric Data - any personal data relating to the physical, physiological, or behavioural characteristics of an individual which allows their unique identification

CEO – Chief Executive Officer

Consent- freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data Subject - a natural person whose personal data is processed by a controller or processor

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

FOI – a freedom of information request for non-personal data.

GDPR – The General data protection regulation. This is an EU law which strengthens the rights of data subjects along with the enforcement powers of the ICO. It comes into force on the 25th May 2018.

ICO – The Information Commissioner's Office. The UK's independent body set up to uphold information rights. It enforces and regulates freedom of information and data protection laws.

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

Right to be Forgotten - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them