Star

NURTURING TODAY'S YOUNG PEOPLE,
INSPIRING TOMORROW'S LEADERS

DATA PROTECTION POLICY

Document control

This document has been approved for operation within:	All Trust Establishments
Date effective from	July 2021
Date of next review	July 2024
Review period	3 Years
Status	Statutory
Owner	Star Academies
Version	7

Contents

Introduction

1. Star Academies collects, processes, holds and shares personal data, and recognises the need to treat it in an appropriate and lawful manner.
2. This policy has due regard to data protection laws, which incorporate the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), and other legal requirements such as the Protection of Freedoms Act 2012.
3. This policy sets out Star requirements for data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.
4. To support this policy, staff shall apply associated policies and procedures[1] and participate in all training if requested to do so by Star.
5. If a member of staff considers that aspects of this policy have not been followed, this should be raised with the Senior Leadership Team of the establishment.
6. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.
7. This policy will be implemented in conjunction with the following Star Academies policies:
    - CCTV Policy
    - Freedom of Information Policy
    - Records Management Policy

Aims

8. To ensure Star Academies fulfils its statutory responsibilities.
9. To ensure effective security and protection for data that has been provided by individuals to Star which is required for the management and operation of its establishments.
10. To support the mission, vision and values of Star Academies and its establishments.

Who is responsible for the policy?

11. Star Academies has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or Star framework. Star Academies has delegated day-to-day responsibility for operating the policy to Star Central, the Local Governing Body and the Head of each establishment.
12. The Local Governing Body and Senior Leadership Team at each establishment has a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

[1] Associated policies and procedures that should be referred to are highlighted in ***bold italics*** within this policy.

Data protection definitions

13. **Data** is information which is stored electronically or in paper-based filing systems.
14. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in the Trust's possession). Personal data can be factual (such as a name, address, date of birth or IP address) or it can be an opinion (such as a performance appraisal).
15. **Special category data** includes information about a person's racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health condition; or sexual orientation and sex life. It also specifically includes the processing of genetic and biometric data. Special category data can only be processed under strict conditions and will usually require the express consent of the person concerned.
16. **Data subjects** are the individuals about whom the personal data is held.
17. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
18. **Biometric data** is personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina, and iris patterns. Within Star Academies, only fingerprints are used.
19. An **Automated biometric recognition system** is a system which measures an individual's physical or behavioural characteristics by using equipment that operates "automatically" (i.e., electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is match in order to recognise the individual.
20. **Data Controller** - Star Academies is registered with the Information Commissioner's Office (ICO Registration Z3350256) as the Data Controller for all of its establishments. As the Data Controller, it determines the purpose for which, and the manner in which, any personal data is processed.

Data protection principles

21. In accordance with the requirements outlined in data protection law, personal data will be:
    - processed lawfully, fairly and in a transparent manner in relation to individuals
    - collected for specific, 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;
    - adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed
    - accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard for the purposes for which it is processed, is erased or rectified without delay

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 law to safeguard the rights and freedoms of individuals
- 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 and organisational measures

22. Star Academies, as the Data Controller, is responsible for, and able to demonstrate, compliance with the principles.
23. In applying data protection law, Star Academies will also apply data protection exemptions that are provided within the law.

Accountability

24. Star Academies, and its establishments, will implement appropriate technical and organisational measures to demonstrate that data is processed in line with data protection law.
25. Star Academies will provide comprehensive, clear and transparent ***Privacy Notices***.
26. A ***Record of Processing*** covering all of Star Academies processing of personal data will be maintained and kept up-to-date annually. This will include the following:
    - Name and details of the organisation
    - Purpose(s) of the processing
    - Description of the categories of personal data
    - Retention schedules
    - Categories of recipients of personal data
    - Description of technical and organisational security measures
    - Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
27. Star Academies, and its establishments, will implement measures that meet the principles of data protection by design and data protection by default, such as:
    - data minimisation
    - pseudonymisation
    - transparency
    - allowing individuals to monitor processing
    - continuously creating and improving security features
28. ***Data Protection Impact Assessments (DPIA)*** are completed when considering using new technologies for the storage, accessing or processing of personal data, or if a new requirement for processing is likely to result in a high risk to the rights and freedoms of individuals.

Data Protection Officer and establishment leads

29. The Star Academies Data Protection Officer (DPO) can be contacted at the following address:

    Head of Governance and Corporate Services

    Data Protection Officer

    Star Academies, Shadsworth Road, Blackburn BB1 2HT

    or Email: regulatory@staracademies.org

30. The duties of the Data Protection Officer include, but are not restricted to:
    - informing and advising the Trust, and its establishments, about their obligations to comply with data protection laws and regulations
    - monitoring compliance with data protection laws and regulations, including managing internal data protection activities, advising on ***Data Protection Impact Assessments (DPIAs)***, managing internal audits, and providing the required training to staff

31. The DPO will operate independently and will not be dismissed or penalised for performing their task.
32. Sufficient resources will be provided to the DPO to enable them to meet the obligations described within data protection law.
33. Data Protection Leads, nominated at each Star Academies establishment, support the DPO. The Head of Establishment shall ensure the role is reflected within the Data Protection Lead's Job Description as follows (and that their responsibility as first point of contact for guidance and support, is known within the establishment):
    - Undertake the role of Data Protection Lead for the Establishment to support the Trust in ensuring compliance as Data Controller under the Data Protection Act
    - In acting as the Data Protection Lead ensure that the Establishment is supported in acting in accordance with Trust Data Protection Policies and Procedures

34. In the event of a data subject looking to exercise their rights, which are listed in this policy, the Data Protection Lead should ensure that these requests are forwarded to the DPO within 24 hours of receipt.

Lawful processing

35. The legal basis for processing data will be identified and documented within the ***Record of Processing*** prior to the data being processed.
36. Data will only be lawfully processed if one of the following conditions is satisfied:
    - Processing is necessary for:
        - compliance with a legal obligation
        - the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
        - for the performance of a contract or to take steps to enter a contract
        - protecting the vital interests of a data subject or another person; or

- the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (this condition is not available to processing undertaken by the establishment in the performance of its tasks)
- The consent of the data subject has been obtained

37. Special category data will only be processed under the following conditions:
    - Explicit consent of the data subject
    - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim, provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
    - Processing relates to personal data manifestly made public by the data subject; or
    - Processing is necessary for:
        - carrying out obligations under employment, social security or social protection law, or a collective agreement
        - protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
        - the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
        - reasons of substantial public interest which is proportionate to the aim pursued and which contains appropriate safeguards
        - the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services or a contract with a health professional
        - reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; or
        - archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes
38. When processing special category data using the following lawful conditions:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services or a contract with a health professional;
    - For reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; or
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

39. Star Academies will meet the requirement to identify an associated condition in UK law, set out in Part 1, Schedule 1 of the Data Protection Act 2018.
40. When processing special category data using the substantial public interest lawful condition, Star Academies will meet one of the 23 specific substantial public interest conditions set out in Part 2, Schedule 1, of the Data Protection Act 2018.

Consent

41. Consent will only be sought prior to processing any data which cannot be done under any other lawful basis, such as complying with a legal or regulatory requirement.
42. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
43. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
44. When seeking consent from pupils, Star Academies will ensure that the pupil understands what they are consenting to and will not exploit any imbalance of power in the relationship between pupils and the Trust.
45. Where consent is given, a ***Consent Record*** will be kept that documents how, when and what type of consent was given.
46. Where the standard of consent cannot be met, processing will cease.
47. Consent provided under previous data protection legislation is reviewed to ensure it meets the standard of current data protection laws. However, acceptable consent obtained under previous data protection legislation will not be reobtained.
48. Consent can be withdrawn by the individual at any time.
49. Where a pupil is capable of understanding their rights under data protection legislation, consent will be gained from the pupil in question.
50. In assessing whether a pupil is capable of understanding and exercising their rights, consideration will be given to the age, maturity, and mental capacity of the pupil in question. Typically, a pupil who is aged 13 or older will be capable of understanding their rights.
51. Consent for the use of photography and video recordings will be taken from the parents/carers of children under the age of 13, as photographs and recordings may be used on Star Academies' websites and social media accounts.
52. If a child under the age of 13 objects to having their photograph taken or appearing in video recordings, and the school deems the pupil to be capable of understanding their rights, then this objection will override any consent provided by the parent/carer.
53. Consent for the use of photography and video recordings will be sought from pupils who are 13 or over, although this is subject to the considerations outlined in point 49 and any safeguarding concerns.
54. In line with the requirements of the Protections of the Freedoms Act 2012, consent for the processing of biometric data will be obtained from parents/carers of children under the age of 18.
55. The consent will be valid for the duration of attendance at that establishment unless consent is withdrawn or there is a notified change of parental responsibility.
56. If there is a disagreement over consent, or if there is no response to a consent request, it will be treated as if consent has not been given.
57. For any pupils classed as 'Looked after Children', or pupils who are adopted, the Designated Safeguarding Lead will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of a LAC pupil, or pupils who are adopted, would risk their security in any way.

The right to be informed

58. A ***Privacy Notice*** is supplied to individuals to provide information on the processing of their personal data. This is written in clear, plain language, which is concise, transparent, easily accessible and free of charge. The ***Privacy Notice*** that is provided to pupils aged 13 and over is written in a clear, plain manner that the child will understand. ***Privacy Notices*** detail all information that is required to be provided to data subjects under data protection laws.
59. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided. This information will be supplied at the time the data is obtained.
60. Where data is not obtained directly from the data subject, information regarding the categories of personal data that Star Academies holds, the source that the personal data originates from and whether it came from publicly accessible sources will be provided. This information will be supplied:
    - if disclosure to another recipient is envisaged, at the latest, before the data is disclosed
    - if the data is to be used to communicate with the individual, at the latest, when the first communication takes place

The right of access

61. Individuals have the right to obtain confirmation that their data is being processed.
62. Individuals have the right to submit a ***Subject Access Request (SAR)*** to gain access to their personal data.
63. A request must be made to the Data Protection Officer. Star Academies also has a ***Subject Access Request Form*** that can be used to ensure all the legally required information is contained within the request.
64. Data Protection Leads at each establishment should forward any ***SARs,*** with the exception of requests for letters from parents of data subjects confirming whether a child is on-roll or in attendance, to the DPO within 24 hours of receipt.
65. Establishments should action requests for letters from parents, staff or other data subjects regarding whether a child is on-roll or in attendance, a member of staff's employment status or other information in line with the ***Dealing with Requests for Letters from Parents, Pupils and Staff Standard Operating Procedure***.
66. If any ***SARs*** are received from parents/carers regarding pupils who are deemed to be capable to understanding their data rights, establishments will seek, and record, the consent of the pupil using the ***Parental Request for Information – Student Consent Form*** before releasing the information.
67. Star Academies is required to verify the identity of the person making the request before any information is supplied.
68. Requests are considered in line with data subject's legal rights and Star Academies' legal obligations.
69. Where a ***SAR*** has been made electronically, the information will be provided in a commonly used electronic format.
70. Any information supplied to the individual will be free of charge. However, Star Academies may impose a fee to comply with requests for further copies of the same information.

71. Where a request is manifestly unfounded, excessive or repetitive, a fee may be charged.
72. All fees will be based on the administrative cost of providing the information.
73. All requests will be responded to without delay and ordinarily within one month of receipt.
74. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
75. Where the request is manifestly unfounded or excessive, Star Academies holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the Information Commissioner's Office (ICO) and to a judicial remedy, within one month of the refusal.
76. In the event that a large quantity of information is being processed about an individual, Star Academies will ask the individual to specify the information the request is in relation to.
77. In England, Wales and Northern Ireland, the parent's automatic right of access to their child's 'educational record' is only applicable in maintained schools and not in academies.
78. Parents are only entitled to access information about their child by making a ***SAR*** if the child is unable to act on their own behalf or has given their consent.

The right to rectification

79. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
80. Where the personal data in question has been disclosed to third parties, Star Academies will inform them of the rectification where possible.
81. Where appropriate, Star Academies will inform the individual about third parties that the data has been disclosed to.
82. Requests for rectification will be responded to within one month. This will be extended by two months where the request for rectification is complex.
83. Where no action is being taken in response to a request for rectification, Star Academies will explain the reason for this to the individual and will inform them of their right to complain to the ICO and to a judicial remedy.

The right to erasure

84. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
85. Individuals have the right to erasure in the following circumstances:
    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
    - When the individual withdraws their consent
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Where are processing of personal data is for direct marketing purposes and the individual objects to that processing
    - The personal data was unlawfully processed
    - The personal data is required 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

86. Star Academies has a right to refuse a request for erasure where the personal data is being processed for the following reasons:
    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
    - The exercise or defence of legal claims
87. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
88. Where personal data has been disclosed to third parties, they will be informed about the erasure of personal data, unless it is impossible or involves disproportionate effort to do so.
89. Where personal data has been made public within an online environment, the establishment will inform other organisations who process the personal data to erase links to and copies of the personal data in question, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

90. Individuals have the right to block or suppress Star Academies' processing of personal data.
91. In the event that processing is restricted, Star Academies will store the personal data, but will not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
92. Star Academies will restrict the processing of personal data in the following circumstances:
    - Where an individual contests the accuracy of the personal data, processing will be restricted until Star Academies has verified the accuracy of the data
    - Where an individual has objected to the processing and Star Academies is considering whether their legitimate grounds override those of the individual
    - Where processing is unlawful and the individual opposes erasure and requests restriction instead
    - Where Star Academies no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim
93. If the personal data in question has been disclosed to third parties, Star Academies will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
94. Star Academies will inform individuals when a restriction on processing has been lifted.

The right to data portability

95. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
96. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
97. The right to data portability only applies in the following cases:
    - To personal data that an individual has provided to a controller; and
    - Where the processing is based on the individual's consent or for the performance of a contract; and
    - When processing is carried out by automated means.
98. Personal data will be provided in a structured, commonly used and machine-readable form.
99. Star Academies will provide the information free of charge.
100. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
101. Star Academies is not required to adopt or maintain processing systems which are technically compatible with other organisations.
102. In the event that the personal data concerns more than one individual, Star Academies will consider whether providing the information would prejudice the rights of any other individual.
103. Star Academies will respond to any requests for portability within one month.
104. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
105. Where no action is being taken in response to a request, Star Academies will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO and to a judicial remedy.

The right to object

106. Star Academies will inform individuals of their right to object at the first point of communication, and this information will be outlined in the ***Privacy Notice*** and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
107. Individuals have the right to object to the following:
    - Processing based on legitimate interests or the performance of a task in the public interest
    - Direct marketing
    - Processing for purposes of scientific or historical research and statistics
108. Where personal data is processed for the performance of a legal task or legitimate interests:
    - An individual's grounds for objecting must relate to his or her particular situation; and
    - Star Academies will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where Star Academies can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

109. Where personal data is processed for direct marketing purposes:
    - Star Academies will stop processing personal data for direct marketing purposes as soon as an objection is received
    - Star Academies cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes

110. Where personal data is processed for research purposes:
    - the individual must have grounds relating to their particular situation in order to exercise their right to object
    - where the processing of personal data is necessary for the performance of a public interest task, Star Academies is not required to comply with an objection to the processing of the data

111. Where the processing activity outlined above is carried out online, Star Academies will offer a method for individuals to object online.

Automated decision making and profiling

112. Individuals have the right not to be subject to a decision when:
    - it is based on automated processing, e.g. profiling; and
    - it produces a legal effect or a similarly significant effect on the individual.

113. Star Academies will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

114. When automatically processing personal data for profiling purposes, Star Academies will ensure that the appropriate safeguards are in place, including:
    - ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact
    - using appropriate mathematical or statistical procedures
    - implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
    - securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

115. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:
    - Star Academies has the explicit consent of the individual
    - the processing is necessary for reasons of substantial public interest

Privacy by design and privacy impact assessments

116. Star Academies will adopt a privacy by design approach and implement technical and organisational measures that demonstrate how Star Academies, and its establishments, have considered and integrated data protection into processing activities.

117. ***Data Protection Impact Assessments (DPIAs)*** will be used to identify the most effective method of complying with Star Academies data protection obligations and meeting individuals' expectations of privacy when new requirements with regards to data processing are identified.

118. ***DPIAs*** will allow Star Academies, and its establishments, to identify and resolve problems at an early stage. This will reduce associated costs, prevent risks to a Data Subjects' rights or damage to the reputation of Star Academies.
119. A ***DPIA*** will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
120. A ***DPIA*** will be used for more than one project, where necessary.
121. High risk processing includes, but is not limited to, the following:
    - Systematic and extensive processing activities, such as profiling
    - Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences; and
    - The use of CCTV
122. Star Academies have a template ***DPIA*** that will be used by its establishments to ensure all required information is included and considered correctly.
123. Establishments will work with the Star Academies Information Governance Lead Adviser to ensure any ***DPIA*** is completed accurately and comprehensively.
124. Where a ***DPIA*** indicates high risk data processing, the matter will be referred to the Data Protection Officer who may consult the ICO in order to seek its opinion as to whether the processing operation complies with data protection laws.
125. Information within the DPIA will assist the completion of the ***Record of Processing***.

Data breaches

126. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
127. The Star Academies Data Protection Officer (DPO), liaising with Data Protection Leads at its establishments, will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their data protection training.
128. All data breaches must be notified immediately to the DPO.
129. A ***Data Breach Reporting Form*** should be used to enable the DPO to have access to all relevant information. However, where all information required is not yet known, this should not delay notification to the DPO. Initial notification may occur whilst further information is gathered by the establishment.
130. Following receipt of the ***Data Breach Reporting Form*** the DPO will complete a ***Breach Risk Assessment Form***, to assist in the decision making regarding whether the matter is required to be reported to the ICO.
131. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be notified.
132. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
133. All ICO notifiable breaches must, by law, be referred to ICO within 72 hours of Star Academies becoming aware of the breach.
134. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Star Academies will notify those concerned directly.

135. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
136. In the event that a breach is sufficiently serious, Star Academies will notify the public without undue delay.
137. Effective and robust breach detection, investigation and internal reporting procedures are required within all Star Academies establishments.
138. Star Academies will maintain a ***Log of Data Protection Breaches***.
139. Failure to report a notifiable breach to ICO without the statutory timescale may result in a fine, as well as a fine for the breach itself.

Security

140. Star Academies will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.
141. Star Academies and its establishments will have in place appropriate procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
142. In line with Star Academies ***Privacy Notices***, we will not share information with third parties without consent unless the law allows us to do so.
143. Personal data shall not be transferred to a country or territory outside of the UK unless that country or territory has a UK "adequacy regulation"[2] or one of the appropriate safeguards, included in the UK GDPR, has been implemented.
144. Personal data will only be transferred to a third-party data processor if that party agrees to comply with Star Academies' policies and procedures on data transfer, including electronic data transfer.
145. Third parties with whom we contract, who will be able to access data as part of that contract, will have to undergo a due diligence check as part of our procurement process. Third parties who do not meet acceptable standards of data security will not be contracted with. If Star Academies becomes aware of any data security concerns regarding a third party with whom we contract, we will reserve the right to terminate the contract.
146. Third parties are only able to access Star Academies ICT systems if they have accepted that they will comply with our ***ICT security policies and procedures***.
147. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:
    - *confidentiality* - only people who are authorised to use the data can access it
    - *integrity* - personal data should be accurate and suitable for the purpose for which it is processed; and
    - *availability* - authorised users should be able to access the data if they need it for authorised purposes

[2] Countries or territories that have a UK adequacy regulation include all EU member states, the three additional EEA member states (Iceland, Norway, and Liechtenstein), Gibraltar, Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (private sector organisations only), and Canada (only data that is subject to Canada's Personal Information Protection and Electronic Documents Act)

148. Security procedures include the following:

- Entry controls are in place and any strangers within entry-controlled areas are reported
- Confidential paper records are kept in locked drawers and cupboards, with restricted access (personal data is always considered confidential)
- Confidential paper records will not be left unattended or in clear view anywhere with general access
- Data users should ensure their PC monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended
- Electronic personal data must be coded, encrypted or password-protected
- Personal data must be stored on the Star Academies network and not individual PCs or other devices
- The Star Academies network drive is regularly backed up off-site
- Where data is required to be saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted
- Electronic devices must be encrypted or password protected and, where possible also enabled to allow the remote blocking or deletion to protect data in case of theft
- Staff and Governors will not store personal data obtained in carrying out their role on their personal devices
- Staff are provided with a secure login and are required to regularly update their password
- Emails containing sensitive or confidential information must be password-protected if there are unsecure servers between the sender and recipient
- Circular emails that contain non-Star email addresses must be sent blind carbon copy (bcc) to prevent the disclosure of email addresses to other recipients
- When sending confidential information by fax, staff must always check that the recipient is present at the receiving machine before sending
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff must take the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the premises accepts full responsibility for the security of the data

149. Before sharing data, all staff will ensure:

- they are allowed to share it
- that adequate security is in place to protect it; and
- the person/organisation who will receive the data has been outlined in a ***Privacy Notice***

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

151. The physical security of the establishment's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to ensure secure data storage will be put in place.

152. Star Academies' Head of ICT is responsible for ensuring continuity and recovery measures are in place to provide for the security of protected data.

153. Star Academies establishments shall ensure that ***ICT security policies and procedures*** are implemented.

Statutory requests for information

154. A statutory request for information is a request for information about a member of staff, pupil or group of pupils from a statutory body.
155. Before information is shared with a statutory body, establishments should ensure they have identified an appropriate lawful basis for processing, or an exemption, and that this is recorded.
156. Star Central have issued guidance regarding how establishments should action and record these requests. Establishments should ensure that they adhere to this guidance outlined in the ***Statutory Request for Information SOP***.

Providing information over the telephone

157. Trust staff dealing with telephone enquiries should take specific precautions to prevent the unlawful disclosure of personal data. In particular they should:
    - verify the caller's identity to ensure information is only given to those legally entitled
    - ensure that any request that falls within the definition of a ***SAR*** follows the correct procedure; and
    - refer to the DPO or the establishment Senior Leadership Team for assistance in difficult situations. No-one should be bullied into disclosing personal information

Publication of information

158. Star Academies has a ***Publication Scheme*** on its websites outlining classes of information that are made routinely available. This includes policies, annual reports and financial information.
159. Classes of information specified on the publication scheme are made available upon request.
160. When uploading information to the Star Academies and establishment websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Images: photography and videos

161. Star Academies understands that recording images of identifiable individuals constitutes processing personal data and should be done in line with data protection principles.
162. Star Academies, and its establishments, notifies all pupils, staff and visitors of the purpose for collecting CCTV images via signage.
163. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
164. CCTV is operated in line with the Trust's ***CCTV Policy***.
165. Star Academies and its establishments will indicate its intentions for taking photographs and/or videos of pupils and will verify permission before publishing them. Consent is sought within the ***Photography and Videos Consent Form***.
166. Under data protection law, photographic images and videos may be kept for archiving purposes, in the public interest and historical research. However, they will not be published within general marketing publications or the website for a period longer than 4 years after the photograph was taken.

167. Where photographic images and/or video is sought for use in a publication not covered within the existing ***Photography and Videos Consent Form***, the ***Photography and Videos Specific Consent Form*** will be used.
168. Images captured by individuals on our premises for recreational/personal purposes, made by parents/carers for family use, are exempt from data protection law.
169. Star Academies provides further advice within their ***Photography and Video Recording SOP*** document.

Biometric information

170. Biometric data is defined as a special category of data under the Data Protection Act 2018 and the UK GDPR.
171. Establishments that are seeking to utilise automated biometric recognition systems (e.g. cashless catering), must contact the Star Academies DPO to advise of their intentions.
172. Prior to processing biometric data or implementing a system that involves processing biometric data, the establishment will work with the DPO to complete a ***DPIA***.
173. Establishments must treat biometric data with appropriate care and comply with legislative requirements under the Protections of Freedoms Act 2012, the Data Protection Act 2018, and the UK GDPR with regard to obtaining consent and the processing of biometric data.
174. Prior to any biometric system being put in place or processing staff biometric data, the establishment will provide staff with the ***Biometric Consent Catering-Staff*** form, or if biometrics are being used for more than one purpose, a ***Biometric Consent Catering and Library*** form. Written consent will be sought from staff regarding the use of biometric systems and the processing of biometric data.
175. Prior to any biometric system being put in place or processing of pupil biometric data, the establishment will send pupils' parents/carers a ***Biometric Consent Catering-Parent*** form, or if biometrics are being used for one than one purpose, a ***Biometric Consent Catering and Library*** form. The written consent of at least one parent/carer must be obtained for a pupil under the age of 18 before any biometric data is processed.
176. The name and contact details of pupil's parents/carers will be taken from the establishment MIS.
177. Where the name of only one parent/carer is included on the establishment MIS, the Principal will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.
178. The establishment does not need to notify a particular parent/carer or seek their consent if it is satisfied that:
    - the parent cannot be found (e.g. their whereabouts or identity is unknown)
    - the parent lacks the mental capacity to object or consent
    - the welfare of the pupil requires that a particular parent is not contacted (e.g. a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts)
    - it is not otherwise reasonably practicable for a particular parent to be notified or for their consent to be obtained

179. Where neither parent of a pupil can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:
    - If a pupil is being looked after by a Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified, and their written consent obtained
    - If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed

180. Star Academies' biometric consent forms sent to staff, parents and other appropriate individuals or agencies will include information regarding the following:
    - Details about the type of biometric data to be taken
    - How the data will be used
    - The staff member's, parent's and pupil's right to refuse and withdraw their consent
    - Reasonable alternative arrangements for those pupils whose data cannot be processed

181. Establishments will not process the biometric data of a pupil under the age of 18 in the following circumstances:
    - The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
    - No parent or carer has consented in writing to the processing
    - A parent/carer has objected in writing to such processing, even if another person has given consent

182. Staff, parents/carers, and pupils can object to participation in the establishment's biometric or withdraw their consent at any time.

183. If a pupil objects or refuses to participate, or continue to participate, in activities that involve the processing of biometric data, the establishment will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parents.

184. In the event of an objection or a withdrawal of consent, any biometric data relating to the member of staff or pupil that has already been captured will be deleted within one month of the date of the objection or withdrawal of consent.

185. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via the ***Biometric Consent Catering-Parent*** or ***Biometric Consent Catering and Library-Parent*** consent forms.

186. Where an individual objects to taking part in the establishment's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service (e.g. where a biometric system is used for cashless catering individuals will be able to use a PIN).

187. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

188. Biometric data will be managed and retained in line with the Star Academies ***Records Management Policy***.

189. Star Academies and its establishments will ensure that robust security measures are implemented to ensure biometric data is protected. These measures will be outlined in a ***DPIA***.

190. Any data breaches concerning an establishment biometric system will be dealt with in line with the data breach procedures described in this policy.

Data retention

191. Data will not be kept for longer than is necessary.
192. Unrequired data will be deleted as soon as practicable.
193. Personal Data will be retained and destroyed in line with the Trust's ***Records Management Policy***.
194. It should be noted that some records relating to former pupils or employees of the establishment may be kept for an extended period for legal reasons, and to enable the provision of references or academic transcripts.
195. Paper and electronic documents/drive memories will be erased or securely destroyed once the data is no longer to be retained.

Disclosure and Barring Service (DBS) data

196. All DBS data will be handled in line with data protection legislation.
197. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.