THE ELTON HIGH SCHOOL

DATA PROTECTION POLICY

Date Prepared	November 2019
Date agreed by Governors	November 2019
Date to be reviewed	November 2020
Person responsible	Daley Thompson

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. The right to rectification
11. The right to erasure
12. The right to restrict processing
13. The right to data portability
14. The right to object
15. Automated decision making and profiling
16. Privacy by design and privacy impact assessments
17. Data breaches
18. Data security
19. Publication of information
20. CCTV and photography
21. Data retention
22. DBS data
23. Biometric Recognition Systems
24. Policy review
25. Appendices

Statement of intent

The Elton High School is required to keep and process certain information about its staff, governors and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The School may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and Governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and The Elton High School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1. Legal framework

1. This policy has due regard to legislation, including, but not limited to the following:

    - The General Data Protection Regulation (GDPR)
    - The Freedom of Information Act 2000
    - The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
    - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
    - The School Standards and Framework Act 1998

2. This policy will also have regard to the following guidance:

    - Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
    - Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. This policy will be implemented in conjunction with the following other school policies:

    - Photographic Images Policy
    - Online Safety Policy
    - Records Management Policy
    - Freedom of Information Policy
    - CCTV Policy

2. Applicable data and Definitions

1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both any automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2. Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act

(DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters. It may also include racial or ethnic origin, political or trade union information, religious belief or sexual orientation.

3. **Processing**. Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

4. **Data subject**. The identified or identifiable individual whose personal data is held or processed.

5. **Data Controller**. A person or organisation that determines the purposes and the means of processing personal data. Our School processes personal data relating to parents, pupils, staff, Governors, visitors and others and therefore is a data controller. The School is registered as a data controller with the ICO and will renew the registration annually or as otherwise legally required.

6. **Data Processor**. A person or other body, other than an employee of the School who processes personal data on behalf of the School.

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

3. Principles

1. In accordance with the requirements outlined in the GDPR, personal data will be:

    - processed lawfully, fairly and in a transparent manner in relation to individuals.
    - 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.
    - adequate, relevant and limited to what is necessary in relation to the purposes 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 are inaccurate, having regard to the purposes for which they are processed, are 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 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.
- 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.

2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

1. The Governing Body of The Elton High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

2. The School will provide comprehensive, clear and transparent privacy policies and when personal data is first collected from individuals, we will provide the relevant information required by data protection law.

3. Additional internal records of the School's processing activities will be maintained and kept up-to-date.

4. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

5. Internal records of processing activities will include the following:

    - name and details of the organisation
    - purpose(s) of the processing
    - description of the categories of individuals and 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

6. The School 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.
7. Data protection impact assessments will be used, where appropriate.
8. The Headteacher acts as the representative of the Data Controller on a day-to day basis.
9. All staff are responsible for:
    - collecting, storing and processing any personal data in accordance with this policy and only processing personal data where it is necessary to do their jobs.
    - informing the School of any changes to their personal data, such as change of address.
    - possibly contacting the DPO in any of the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - with any concerns that this policy is not being followed.
    - if there is lack of sureness whether or not they have a lawful basis to use personal data in a particular way.
    - if there is a need to rely on or capture consent, draft a privacy notice, deal with data protection rights or transfer personal data outside the European Economic Area.
    - if there has been a data breach.

- if involved in a new activity that may affect the privacy rights of individuals.
- if help is required with contracts or sharing personal data with third parties.

In all of the above circumstances, advice from the School Data Manager should be sought as a first step.

Regular training for all members of staff will be provided on data protection law, this policy, any related policies and other data protection matters as identified. Records of attendance will be kept for such training.

5. Data protection officer (DPO)

1. A DPO will be appointed in order to:
    - inform and advise the School and its employees about their obligations to comply with the GDPR and other data protection laws.
    - monitor the School's compliance with the GDPR and other laws, including reviews, managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
2. An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
4. The DPO will report to the highest level of management at the School, which is the **Headteacher and The Governing Board**.
5. The DPO will operate independently and will not be dismissed or penalised for performing their task.
6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

1. The legal basis for processing data will be identified, adhered to and documented prior to data being processed.

2. Under the GDPR, data will be lawfully processed under the following conditions:

    - the consent of the data subject has been obtained.

   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 with the data subject or to take steps to enter into a contract.
    - protecting the vital interests of a data subject or another person.
    - for the legitimate purposes pursued by the School 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 School in the performance of its tasks.)
    - the School, as a public authority, can perform a task, in the public interest and carry out its official functions.

3. Sensitive data will only be processed under the following conditions:

    - explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
    - 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.

   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 on the basis of Union or Member State law 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 or treatment or management of health or social care systems and services on the basis of Union or Member State law 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.
- archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
3. Where consent is given, a record will be kept documenting how and when consent was given.
4. The School ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
6. Consent can be withdrawn by the individual at any time.
7. Where a child is under the age of 16 or younger if the law provides it (upto the age of 13), the consent of parents will be sought prior to the processing of their

data, except where the processing is related to preventative or counselling services offered directly to a child.

8. Whenever we first collect personal data from individuals, we will provide them with the relevant information required by data protection law.

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

    - there is an issue with a pupil or parent/carer that causes a safety risk.
    - there is a need to liaise with other agencies – we will seek consent prior to this.
    - School suppliers, online services/applications or contractors need data to provide services to staff and pupils. Suppliers and contractors used must guarantee they can comply with data protection law and an agreement will be established, ensuring the fair and lawful processing of any data shared. Only data shared will be that required to carry out services.
    - there is a need to share data with law enforcement / government bodies, where we are legally required to do so, including for:
    - prevention or detection of crime or fraud.
    - apprehension or prosecution of offenders.
    - assessment or collection of tax owed to HMRC.
    - legal proceedings
    - safeguarding obligations require such action.
    - research / statistical purposes following consent or anonymisation.
    - in the case of emergency affecting members of the School community with, emergency services and the Local Authority.

8. <u>The right to be informed</u>

1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. They are found on the School's website and also in the appendices of this policy.

2. If services are offered directly to a child, the School will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

    - the identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
    - the purpose of, and the legal basis for, processing the data.
    - the legitimate interests of the controller or third party.
    - any recipient or categories of recipients of the personal data.
    - details of transfers to third countries and the safeguards in place.
    - the retention period of criteria used to determine the retention period.
    - the existence of the data subject's rights, including the right to:
    - withdraw consent at any time.
    - lodge a complaint with a supervisory authority.
    - lodge a complaint to prevent processing that is likely to cause damage or distress.
    - the existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

4. 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.

5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- within one month of having obtained the data.
- if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- if the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

1. Individuals have the right to obtain confirmation that their data is being processed and its type and purpose, who it has been or will be shared with and how long it will be retained for.
2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Any SAR received must be immediately forwarded to the School Data Manager, who will liaise with the DPO as needed.
3. The School will verify the identity of the person making the request and the source of the data, before any information is supplied.
4. A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.
5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
7. All fees will be based on the administrative cost of providing the information.
8. All requests will be responded to without delay and at the latest, within one month of receipt. Refusals should provide the reason and right to complain to the ICO.
9. 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.
10. Where a request is manifestly unfounded or excessive, the School 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 supervisory authority and to a judicial remedy, within one month of the refusal.

11. In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

12. Personal data about a child belongs to that child and SARs would normally be subject to the consent of the child. Children aged 13 or above are generally regarded to be mature enough to understand their rights with cases judged on an individual basis. Parents/carers have a legal right of access to their child's educational record including most information.

13. Grounds for refusal to disclose information include: the potential to cause harm to the physical or mental health of the pupil or another; where there is risk of abuse; information is contained in adoption records or given to a court in proceedings involving the child.

10. The right to rectification

1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

2. Where the personal data in question has been disclosed to third parties, the School will inform them of the rectification where possible.

3. Where appropriate, the School will inform the individual about the third parties that the data has been disclosed to.

4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

5. Where no action is being taken in response to a request for rectification, the School will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

2. 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

- 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

3. The School has the 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
4. 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.
5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
6. Where personal data has been made public within an online environment, the School will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. <u>The right to restrict processing</u>

1. Individuals have the right to block or suppress the School's processing of personal data.
2. In the event that processing is restricted, the School will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
3. The School 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 the School has verified the accuracy of the data
- where an individual has objected to the processing and the School 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 the School no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

4. If the personal data in question has been disclosed to third parties, the School will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
5. The School will inform individuals when a restriction on processing has been lifted.

13. <u>The right to data portability</u>

1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
2. 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.
3. The right to data portability only applies in the following cases:
    - to personal data that an individual has provided to a controller
    - where the processing is based on the individual's consent or for the performance of a contract
    - when processing is carried out by automated means
4. Personal data will be provided in a structured, commonly used and machine-readable form.
5. The School will provide the information free of charge.
6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

7. The School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

8. In the event that the personal data concerns more than one individual, the School will consider whether providing the information would prejudice the rights of any other individual.

9. The School will respond to any requests for portability within one month.

10. 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.

11. Where no action is being taken in response to a request, the School 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 supervisory authority and to a judicial remedy.

14. <u>The right to object</u>

1. The School 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.

2. 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.

3. 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.
    - the School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the School can demonstrate

compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

4. Where personal data is processed for direct marketing purposes:
    - the School will stop processing personal data for direct marketing purposes as soon as an objection is received.
    - the School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
5. 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, the School is not required to comply with an objection to the processing of the data.
6. Where the processing activity is outlined above, but is carried out online, the School will offer a method for individuals to object online.

15. Automated decision making and profiling

The Elton High School does not engage in automated decision making or profiling. The only exception to this is the use of pupil fingerprints to receive school lunch instead of paying with cash. This is clearly optional and requires parental consent, which may be withdrawn at any time. Information held is not portable to any other IT environment, only being retained for the period of attendance of the pupil at the School.

16. Privacy by design and privacy impact assessments

1. The School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the School has considered and integrated data protection into processing activities.
2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the School's data protection obligations and meeting individuals' expectations of privacy.
3. DPIAs will allow the School to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the School's reputation which might otherwise occur.

4. 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.

5. A DPIA will be used for more than one project, where necessary.

6. 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
    - the use of CCTV.

7. The School will ensure that all DPIAs include the following information:

    - a description of the processing operations and the purposes
    - an assessment of the necessity and proportionality of the processing in relation to the purpose
    - an outline of the risks to individuals
    - the measures implemented in order to address risk

8. Where a DPIA indicates high risk data processing, the School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. <u>Data breaches</u>

1. 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.

2. The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the School becoming aware of it.

5. 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.

6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the School will notify those concerned directly.

7. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the School, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

10. Within a breach notification, the following information will be outlined:

    - the nature of the personal data breach, including the categories and approximate number of individuals and records concerned
    - the name and contact details of the DPO
    - an explanation of the likely consequences of the personal data breach
    - a description of the proposed measures to be taken to deal with the personal data breach
    - where appropriate, a description of the measures taken to mitigate any possible adverse effects

11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. <u>Data security</u>

1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

4. Where data is 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.

5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

6. All electronic devices are password-protected to protect the information on the device in case of theft.

7. Where possible, the School enables electronic devices to allow the remote blocking or deletion of data in case of theft.

8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients or using the Schools SIMS InTouch email service.

11. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the School premises accepts full responsibility for the security of the data.

13. Before sharing data, all staff members will ensure:

    - they are allowed to share it.
    - that adequate security is in place to protect it.
    - who will receive the data has been outlined in a privacy notice.

14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the School containing sensitive information are supervised at all times.

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

16. The Elton High School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17. The School Business Manager and School Data Manager are responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Publication of information

1. The Elton High School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
    - Policies and procedures
    - minutes of meetings
    - annual reports
    - financial information
2. Classes of information specified in the publication scheme are made available quickly and easily on request.
3. The Elton High School will not publish any personal information, including photos, on its website without the permission of the affected individual.
4. When uploading information to the School website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV and photography

1. The School uses CCTV in various locations to support the safety of pupils, staff and visitors. We will adhere to the ICO Code of Practice for the use of CCTV.
2. The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
3. Security cameras are clearly visible and all pupils, staff and visitors are advised that cameras are in use through prominent signs.
4. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
5. All CCTV footage will be kept for 31 days for security purposes; the School Business Manager is responsible for keeping the records secure and allowing access. Enquiries relating to the CCTV system should be referred to the School Business Manager.
6. As part of School activities we may take photographs and record images of individuals in our School. Uses may include notice board displays, School publications, the School website or out of School through newspapers/ social media.

7. The School will always explain the purpose for taking photographs of pupils and will ensure parental permission before publishing them. Consent to this can be refused or withdrawn at any time.

8. If the School wishes to use images/video footage of pupils in a publication, such as the School website, prospectus, or recordings of School plays, written permission will be sought for the particular usage from the parent of the pupil.

9. Precautions, as outlined in the School Photographic Images Policy, are taken when publishing photographs of pupils, in print, video or on the School website. As a general rule, pupils will not be identifiable in this situation and images will not be accompanied by any personal information.

10. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21. <u>Data retention</u>

1. Records will be kept and disposed of in line with the School Records Management Policy.

2. Data will not be kept for longer than is necessary.

3. Unrequired data will be deleted as soon as practicable.

4. Some educational records relating to former pupils or employees of the School may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

5. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. We may use a third party to securely dispose of record material, under requirement that the third party complies with data protection law.

22. <u>DBS data</u>

1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

2. Data provided by the DBS will never be duplicated.

3. 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.

23. Biometric recognition systems

Where pupil biometric data is part of an automated biometric recognition system – for instance the use of fingerprints to receive School lunch instead of paying with cash, we will comply with the Freedom of Information Act 2012. Written consent from parents prior to participation is required and the alternative use of cash is available. Consent for this function can be withdrawn at any time.

24. Policy review

1. This policy is reviewed annually by the DPO and School Data Manager with recommendations reported to the Headteacher.

2. The next scheduled formal review date for this policy is **December 2021**.

Appendix A – Privacy Notice – How we use pupil information

- **Why do we collect and use pupil information?**

  We collect and use pupil information under Article 6(1)(b) '*Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract,'* and article 9(2)(b) '*Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.'*

  We use the pupil data:

  - **(a)** to support pupil learning
  - **(b)** to monitor and report on pupil attainment and progress
  - **(c)** to provide appropriate pastoral care
  - **(d)** to support and assess the quality of our services
  - **(e)** to keep children safe (food allergies, or emergency contact details)
  - **(f)** to meet the statutory duties placed upon us.

  Under the General Data Protection Regulation (GDPR) Article 9, the lawful bases we rely on for processing pupil information are:

  - for the purposes of **(a), (b), (c)** &**(d)** in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function
  - for the purposes of **(e)** in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)
  - for the purposes of **(f)** in accordance with the legal basis of Legal obligation: data collected for DfE census information
    - Section 537A of the Education Act 1996
    - the Education Act 1996 s29(3)
    - the Education (School Performance Information)(England) Regulations 2007
    - regulations 5 and 8 School Information (England) Regulations 2008
    - the Education (Pupil Registration) (England) (Amendment) Regulations 2013

  In addition, concerning any special category data:

  - conditions a, b, c and d of GDPR - Article 9

  What is your 'Personal Data'?

  Personal data is information that says something about you as an individual, so it would normally include your name, and/or contact details, or even a photograph of you.

The categories of parent information that we collect and hold include:

- Personal information (names, addresses, contact numbers, email addresses, relationship to pupil).

The categories of pupil information that we collect, hold and share include:

- Personal information (name, unique pupil number, date of birth, address, photograph, and religion)
- Characteristics (ethnicity, language, nationality, country of birth, catering and free school meal eligibility, biometrics)
- Safeguarding information (such as court orders and professional involvement)
- Education Information (Previous school(s), Special Educational Needs Information (including the needs and ranking), National Curriculum Assessment results, Post 16 learning information, information for certain trips and/or activities)
- Medical and administration (such as doctor's information, child health, dental health, allergies, medication and dietary requirements)
- Attendance information (sessions attended, number of absences and absence reasons, exclusions/behavioural information)
- Welfare (In care details, child protection plans)

Collecting pupil information

We obtain pupil information via registration forms at the start of year 7. In addition, when a child joins us from another school, we are sent a secure file (Common Transfer File (CTF)) containing relevant information. Also, we can collect data from medication forms and from child protection plans.

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data securely until the pupil reaches the age of 25. Images of pupils used on the School website to promote the School will be removed 3 years after the pupil has left.

Who do we share pupil information with?

We routinely share pupil information with:

- Schools/educational organisations that pupils attend after leaving us
- outside agencies
- our local authority
- youth support agencies (pupils aged 13+)

- the Department for Education (DfE)

Why we routinely share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Youth support services

What is different about pupils aged 13+?

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the pupil's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once he/she reaches the age of 16.

Aged 14+ qualifications

For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications.

Our pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website http://www.bury.gov.uk/index.aspx?articleid=10386.

Department for Education

We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information)(England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under GDPR, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mr D Thompson (Data Protection Officer) thompsond@eltonhigh.bury.sch.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with the School in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:

- Mr D Thompson (Data Manager) – thompsond@eltonhigh.bury.sch.uk
- Mr Neil Scruton (Data Protection Officer) - scrutonn@eltonhigh.bury.sch.uk
- Bury Local Authority

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of pupils and their characteristics in each school.
- informs 'short term' education policy monitoring (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy. (for example, how certain subject choices go on to affect education or earnings beyond school)

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law to provide information about our pupils to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the Department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

Sharing

The Department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact the DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, the DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: https://www.gov.uk/contact-dfe

Appendix B – Privacy Notice – The school Workforce

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, our School. This is for employment purposes to assist in the running of the School and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names, date of birth, gender, disabilities, and National Insurance numbers and characteristics such as ethnic group, Qualified Teacher Status, employment contracts and remuneration details, qualifications, absence information, and curriculum details.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

- http://www.bury.gov.uk/index.aspx?articleid=10637
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

- Neil Scruton (EHS DPO) - scrutonn@eltonhigh.bury.sch.uk
- Daley Thompson (EHS Data Manager) – thompsond@eltonhigh.bury.sch.uk

Appendix C – Privacy Notice – The School Governors

The Elton High School is the data controller for Governor information.

1.1 The categories of Governor information that we process include:

- personal identifiers, contacts and characteristics (such as name, date of birth, contact details and postcode)
- governance details (such as role, start and end dates and Governor ID)

Why we collect and use Governor information

The personal data collected is essential, in order for the School to fulfil their official functions and meet legal requirements.

We collect and use Governor information for the following purposes:

a) to meet the statutory duties placed upon us

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

- for the purpose **a)** named above in accordance with the legal basis of legal obligation.

All maintained school governing bodies, under section 538 of the Education Act 1996 and academy trusts, under the Academies Financial Handbook have a legal duty to provide the governance information as detailed above.

In addition, concerning any special category data:

- conditions a, b, c, and d of GDPR - Article 9

Collecting Governor information

We collect personal information via a data collection form when they start and it is checked and updated regularly.

Governor data is essential for the School's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it may be requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing Governor information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit http://www.eltonhigh.bury.sch.uk/school-information/policies.

Who we share Governor information with

We routinely share this information with:

- our local authority (where applicable)
- the Department for Education (DfE)

Why we share Governor information

We do not share information about our Governors with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are legally required to share information about our Governors with our local authority (LA). Further details in relation to this are available from Bury Local Authority. Appropriate security measures for information indicated are provided by Bury Local Authority.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities.We are required to share information about our Governors with the Department for Education (DfE), under:section 538 of the Education Act 1996

All data is entered manually on the GIAS system and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact **Daley Thompson (Schools Data Manager) thompsond@eltonhigh.bury.sch.uk or Neil Scruton (Schools Data Protection Officer) scrutonn@eltonhigh.bury.sch.uk**

Under certain circumstances you also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

- **Neil Scruton (Schools Data Protection Officer)** **scrutonn@eltonhigh.bury.sch.uk**
- **Daley Thompson (Schools Data Manager)** **thompsond@eltonhigh.bury.sch.uk**

How Government uses your data

The Governor data that we lawfully share with the DfE via GIAS:

- will increase the transparency of governance arrangements
- will enable schools and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context
- allows the department to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role

Data collection requirements

To find out more about the requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Note: Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to a small number of DfE staff who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless the law allows it.

Appendix D – Subject Access Request (SAR) record

Subject access request record

Name of data subject: _____
Name of person who made request: _____
Date request received: ___/___/____
Contact DPO: ___/___/____
Date acknowledgement sent: ___/___/____
Name of person dealing with request: _____

	Notes (overwrite the statements in grey)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data.	What data sources, where are they kept
Collect the data required.	You may need to ask others - state a deadline in your request
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as the Psychology Service, we do not own the data.
Do you need to except/redact data?	If exempting/redacting be clear of your reasons. Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reasons for delay and asking if they would like the data you have collected so far.
Create pack.	Make sure that the data is in an easy to access format: paper, word, excel (csv), etc. Make a copy to keep.
Inform requestor you have the data.	Ask them how they would like it delivered.
Deliver data.	Ask for confirmation/special delivery?

At all stages, your DPO will be able to provide you with advice

Date request completed: ___/___/____
(within 30 days of request)

Appendix E – Letter Template for refusal of a SAR

…./……/20…….

Dear ……..

I am writing to you to let you know your request for information from The Elton High School relating to……. requested on ……/……../20….. has been denied.

We have denied access to this information because
……
……
……

Please be aware that if you are not satisfied with the reasons listed above, and you would like to discuss this matter further, please contact School.
In addition, you have the right to complain to the Information Commissioner's Office (ICO) and also to seek judicial remedy, if you so wish.

Yours sincerely

Neil Scruton
Data Protection Officer
scrutonn@eltonhigh.bury.sch.uk

Daley Thompson
Data Manager
thompsond@eltonhigh.bury.sch.uk