SCHOOL POLICY

Turton School

GDPR Data Protection Policy

Reviewed by:	Resources Committee
Signed (Governing Board):	
Date:	October 2022
Next Review due:	October 2025

Produced by Turton School

Statement of intent

Turton School is required to keep and process certain information about its staff members 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 core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and **Turton 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 will come 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.

Signed by:

_____ Head Teacher Date: _____

_____ Chair of governors Date: _____

Legal framework
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

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'

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

- **Privacy notices (staff & students)**
- **Online Safety School Policy**
- **CCTV Policy**
- **Personal Data Log**

Applicable data
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 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.

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.

Principles
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.

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

Accountability
Turton School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

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.

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 parties, including documentation of the transfer mechanism safeguards in place

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.
- Data protection impact assessments will be used, where appropriate.

Data protection officer (DPO)
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 managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will 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.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Head Teacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful processing
The legal basis for processing data will be identified and documented prior to data being processed. Details can be found in the Personal Data Log.

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 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 school in the performance of its tasks.)

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).

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

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.

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.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 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.

The right to be informed

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.

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.

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.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

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.

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.

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

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.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.

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.

The school will verify the identity of the person making the request before any information is supplied.

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.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt. 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. 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.

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.

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under

the age of 12, The primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

Under the Education (Pupil Information) (England) Regulations 2005, a parent has the right to access their child's educational record.

Under the Regulations, requests from parents to view their child's educational record will be dealt with by the Board of Governors. All other requests for personal information from the pupil, or someone acting on their behalf, will be dealt with by the Head Teacher on behalf of the school.

A SAR form can be found in appendix 3.

The right to rectification
Individuals are entitled to have any inaccurate or incomplete personal data rectified.

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

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

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

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.

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

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

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

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.

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.

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.

The right to restrict processing
Individuals have the right to block or suppress the school's processing of personal data.

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.

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

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.

The school will inform individuals when a restriction on processing has been lifted.

The right to data portability
Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

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.

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

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

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

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.

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

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.

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.

The right to object
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.

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.

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.

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.

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.

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

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

The school 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.

When automatically processing personal data for profiling purposes, the school 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.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:
- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

Privacy by design and privacy impact assessments
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.

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.

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.

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.

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

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.

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

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.

Data breaches

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.

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

A flow chart detailing procedures for identifying and reporting a data breach is included in **Appendix 5**

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

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

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.

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.

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

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

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.

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

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

Records will be maintained of any suspected breaches of information security using the form attached in **Appendix 2.**

The form will be completed in the event of loss of unauthorised disclosure of information. The details of the incident will be used to create a correctional action plan to ensure that a similar incident does not happen again.

Following a reported incident, the school will investigate and after liaising with the Local Authority decide if the incident is of sufficient severity to report to The Information Commissioners Office.

Data security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Confidential data is not displayed on walls etc. where non authorised staff/students/visitors can see it.
  NB – display of confidential data could include student photos with name and form details.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up to a separate site building.
- 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.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Staff lock their computers when they are not in the room.
- Staff do not access confidential information on their computer when non authorised staff /students/visitors can see the screen.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- The Council Egress system is used for sending confidential information to the Local Authority.
- Circular emails to parents are sent via Teachers2Parents so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.

- Staff and governors who use their personal laptops, computers, iPads etc. for school purposes will ensure that personal data is accessed via the School's Remote Access system or will follow the security procedures detailed below:
  Security procedures - 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 adhere to the following procedures for security, i.e:
  - The data is kept secure under lock and key.
  - Electronic devices are password protected
  - The data is kept private and not viewed in a public area or where friends/family etc. can view the data.
  - The data is returned to School premises or destroyed as soon as possible.
  - The data is removed from electronic devices and stored on the School's network as soon as possible.
  - Where staff wish to work using a cloud based platform then the IT department must set up the required area. Personal ICloud, Google Drive accounts etc. must not be used
  - The person taking the information from the school premises accepts full responsibility for the security of the data.
- 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 is detailed in the School's privacy notices which can be found on the school website.
  - The Data Protection Officer has been informed of the data sharing.
    NB – Sharing data includes saving data to online platforms such as MyMaths etc. Where any personal staff or pupil data is entered onto a system separate to the school then this is defined as sharing of data.
- 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.
- 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.
- Turton School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Network Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.
- The school will introduce a protective marking scheme to ensure that all data – electronic or on paper – is labelled according to the protection it requires based on Impact Levels:

Impact level	**Impact**	**Colour Code**	**Memory stick?**	**Example**
IL0–Not Protectively Marked	No harm or embarrassment will occur if items become public knowledge		Yes	Newsletters, public information
IL1- Unclassified			Yes	Generic letters to parents containing no personal data

IL2–PROTECT	Some harm or embarrassment will occur if items become public knowledge		No	Basic student information such as name and address
IL3–Restricted	Harm or embarrassment will occur if items become public knowledge		No	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential	Serious harm or embarrassment will occur if items become public knowledge		No	Highly sensitive student data relating to child protection

An Information Risk Register will be created and maintained by the school which summarises each information asset the school maintains. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned. The information risk register can be found in **Appendix 1.**

Publication of information
Turton School will not publish any personal information, including photos, on its website without the permission of the affected individual.

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.

Personal information to 3rd parties

a. Information sharing with professionals working with children

Information sharing between professionals is vital to ensure the wellbeing of Children. The school will follow the "7 golden rules of Information Sharing" described by the DfE:

- Remember that the GDPR is not a barrier to sharing information
- Be open and honest with the person or family
- Seek advice if you are in any doubt
- Share with consent where appropriate
- Consider safety and well-being
- Necessary, proportionate, relevant, accurate timely, and secure
- Keep a record of your decision and reasons
- Unauthorised disclosure of personal data is a criminal offence and will likely lead to disciplinary action

b. Investigation of a crime
The school will treat requests for information from an official bodies related to criminal or taxation purposes under The Law Enforcement Directive. The school requires the requestor to complete the Request for Personal Data form (Appendix 4).

Requests from the police will be countersigned by a person no lower than inspector. For requests from other organisations other than the police, the form will be countersigned by a person of a higher position within the organisation than the person making the request.

The decision re access will be made by the Head teacher. Generally, the school reserves the right not to release the data but there may be situations such as the receipt of a court order that requires the school to release the information.

CCTV and photography
The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for three months for security purposes; the ICT Manager is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

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.

Precautions are taken when publishing photographs of pupils, in print, video or on the school website.

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

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

Unrequired data will be deleted as soon as practicable.

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.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

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

Data provided by the DBS will never be duplicated.

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.

Disclosure of non - personal information / FOI Requests
The school as a public authority is subject to The Freedom of Information Act 2000 and all requests for information that is not personal information must be treated as a Freedom of Information request. FOI requests must be fully responded within 20 (school) working days by

law. The information will be provided unless the school can provide an exemption under the FOI act.

Policy review
This policy is reviewed every three years by the SBM and the Head Teacher.
The next scheduled review date for this policy is **October 2025.**

Appendix 1
Information Risk Register

This retention schedule is based on guidance from the records management society:
http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf

Information Asset Owners are responsible for:
1 Ensuring the information is used for the purpose it was collected
2 How information has been amended or added to over time
3 Who has access to protected data and why

Named Information Asset Owners are:

HT	Head Teacher
DH (P)	Deputy Head Pastoral – Cathy Bach
DHO	Deputy Head Operations – Carole Baily
CtG	Clerk to Governors
SBM	School Business Manager - Leonie Hathaway
HR	HR Manager – Leonie Hathaway
IND	Individual staff
PS	Pastoral secretary
DM	Data Manager
SEN	Senco
EO	Exams Officer
EVC	Educational Visits Coordinator
BC	Bolton Council

1 Child Protection

These retention periods should be used in conjunction with the document "Safeguarding Children and Safer Recruitment in Education which can be downloaded from this link:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289214/safeguarding_children_and_safer_recruitment_in_education.pdf

IAO	Basic file description	Data Prot Issues	Statutory Provisions	Retention period [operational]	Action at the end of the administrative life of the record	Protective Marking Classification
DH (P)	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years	SECURE DISPOSAL Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)	**IL4-Confidential**
DH (P)	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60 "Record Keeping 5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."	**IL4-Confidential**

2 Governors						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
	Minutes					
CtG	*Principal set (signed)*	No		Permanent	Retain in school whilst school is open then transfer to Archives.	**IL3 - RESTRICTED**
CtG	*Inspection copies*	No		Date of meeting + 3 years	If these minutes contain any sensitive personal information they should be SECURELY DISPOSED	**IL3 - RESTRICTED**
CtG	Agendas	No		Date of meeting	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Reports	No		Date of report + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Annual Parents' meeting papers	No		Date of meeting + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
CtG	Instruments of Government	No		Permanent	Retain in school whilst school is open then transfer to Archives.	**IL1–Unclassified**
SBM	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required then transfer to Archives.	**IL1–Unclassified**
HT	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL	**IL1–Unclassified**

CtG	Statutory Policy documents (does not include school specific policies such as writing policies etc.)	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process) SECURE DISPOSAL	**IL1–Unclassified**
HT	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years. Review for further retention in the case of contentious disputes. SECURE DISPOSAL	**IL3 - RESTRICTED**

3 Management						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
CtG	Minutes of the Senior Management Team and other internal administrative bodies	Yes[1]		Date of meeting + 5 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
CtG	Reports made by the head teacher or the management team	Yes[1]		Date of report + 3 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
IND	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**

IND	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
CtG	Professional development plans (Management plans for professional development plans of staff)	Yes		Closure + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
CtG	School development plans	No		Closure + 6 years	Review Offer to the Archives	**IL2–PROTECT**
PS	Admissions – if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
PS	Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**

PS	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
PS	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL	**IL3 - RESTRICTED**
[1] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.						
PS	Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry. Offer to the Archives	**IL3 - RESTRICTED**
DM	Attendance registers	Yes	The Education (Pupil Registration) (England) Regulations 2006 (No. 1751)	Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]	**IL3 - RESTRICTED**
DM	Pupil record cards	Yes	Limitation Act 1980	DOB of the pupil + 25 years[1]	SECURE DISPOSAL	**IL3 - RESTRICTED**
DM	Pupil files	Yes	Limitation Act 1980	DOB of the pupil + 25 years[2]	SECURE DISPOSAL	**IL3 - RESTRICTED**

SEN	Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years	SECURE DISPOSAL NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	**IL4-Confidential**
PS	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL	**IL2–PROTECT**
EO	Examination results - Public	No		Year of exams + 6 years	SECURE DISPOSAL Any certificates left unclaimed should be returned to the appropriate Examination Board	**IL2–PROTECT**
DHO	Internal examination results	Yes		Current year + 5 years[3]	SECURE DISPOSAL	**IL2–PROTECT**
HT	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL	**IL3 - RESTRICTED**
SEN	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**

SEN	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
SEN	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**
SEN	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending	**IL3 - RESTRICTED**
SEN	Children's SEN Files	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SECURE DISPOSAL unless legal action is pending	**IL4-Confidential**

EVC	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL	**IL3 - RESTRICTED**
EVC	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL	**IL3 - RESTRICTED**
EVC	Records created by schools to obtain approval to run an Educational Visit outside the Classroom	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years[7]	SECURE DISPOSAL or delete securely	**IL2–PROTECT**

[1] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

[2] As above

[3] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

[4] This retention period has been set in agreement with the Safeguarding Children's Officer

4 Curriculum						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
DHO	Curriculum development	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
DHO	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL	**IL1–Unclassified**
DHO	School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**
DHO	Schemes of work	No		Current year + 1 year This retention period starts once the document has been superceded	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**
DHO	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL1–Unclassified**
IND	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**

IND	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
IND	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
IND	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL	**IL2–PROTECT**
DHO	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DHO	SATS records	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DHO	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
DHO	Value added records	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
HT	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**

5 Personnel Records held in Schools						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
HR	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
HR	Staff Personal files	Yes		Permanent	SECURE DISPOSAL	**IL2–PROTECT**
HR	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL	**IL2–PROTECT**
HR	Pre-employment vetting information (including DBS Checks)	No	DBS Guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]	**IL2–PROTECT**
HR	Single Central Record	Yes	ISA guidelines	Keep until school closure	Offer to local authority designated officer	**IL2–PROTECT**
HR	Disciplinary proceedings:		**Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter, please contact your safeguarding children officer for further advice.**			
HR	*verbal warning*	Yes		Date of warning + 6 months	SECURE DISPOSAL	**IL2–PROTECT**
HR	*written warning – level one*	Yes		Date of warning + 6 months	SECURE DISPOSAL	**IL2–PROTECT**

HR	*written warning – level two*	Yes		Date of warning + 12 months	SECURE DISPOSAL	**IL2–PROTECT**
HR	*final warning*	Yes		Date of warning + 18 months	SECURE DISPOSAL	**IL2–PROTECT**
HR	*case not found*	Yes		If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case		**IL2–PROTECT**
HR	Records relating to accident/injury at work	Yes		Date of incident + 12 years	In the case of serious accidents a further retention period will need to be applied. SECURE DISPOSAL	**IL2–PROTECT**
CtG	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL	**IL2–PROTECT**
BC	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL	**IL2–PROTECT**
BC	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SECURE DISPOSAL	**IL2–PROTECT**

BC	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
HR	Proof of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes			Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file.	**IL2–PROTECT**
[1] If this is placed on a personal file it must be weeded from the file.						

6 Health and Safety						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
BM	Accessibility Plans	No	Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
BM	*Adults* *(All Accidents)*	Yes		Date of incident + 7 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
BM	*Children* *(All Accidents)*	Yes		DOB of child + 25 years[1]	SECURE DISPOSAL	**IL3 - RESTRICTED**
BM	COSHH	No		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECURE DISPOSAL	**IL1–Unclassified**
BM	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
BM	Policy Statements	No		Date of expiry + 1 year	SECURE DISPOSAL	**IL1–Unclassified**
BM	Risk Assessments	No		Current year + 3 years	SECURE DISPOSAL	**IL1–Unclassified**

BM	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No		Last action + 40 years	SECURE DISPOSAL	**IL1–Unclassified**
RS	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No		Last action + 40 years	SECURE DISPOSAL	**IL1–Unclassified**
BM	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**

[1] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

7 Administrative						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
BM	Employer's Liability certificate	No		Closure of the school + 40 years	SECURE DISPOSAL	**IL1–Unclassified**
BM	Inventories of equipment and furniture	No		Current year + 6 years	SECURE DISPOSAL	**IL1–Unclassified**
BM/ HR	General administrative records (records not specifically listed elsewhere)	No		Current year + 5 years	Review to see whether a further retention period is required	**IL1–Unclassified**
CtG	School brochure or prospectus	No		Current year + 3 years		**IL1–Unclassified**
HR	Circulars (staff/parents/ pupils)	No		Current year + 1 year	SECURE DISPOSAL	**IL1–Unclassified**
HR	Newsletters, ephemera	No		Current year + 1 year	Review to see whether a further retention period is required	**IL1–Unclassified**
HR	Visitors book	No		Current year + 2 years	Review to see whether a further retention period is required	**IL1–Unclassified**
DHP	PTA/Old Pupils Associations	No		Current year + 6 years	Review to see whether a further retention period is required	**IL1–Unclassified**

8 Finance						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
BM	Annual Accounts	No	Financial Regulations	Current year + 6 years	Offer to the Archives	**IL2–PROTECT**
BM	Loans and grants	No	Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	**IL2–PROTECT**
	Contracts					
BM	under seal	No		Contract completion date + 12 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	under signature	No		Contract completion date + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	monitoring records (Bolton Council Corporate Property Unit may hold these records on the schools behalf)	No		Current year + 2 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Copy orders	No		Current year + 2 years	SECURE DISPOSAL	**IL2–PROTECT**

BM	Budget reports, budget monitoring etc	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Invoice, receipts and other records covered by the Financial Regulations	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Annual Budget and background papers	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Order books and requisitions	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Delivery Documentation	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Debtors' Records	No	Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – Cheque books	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – Paying in books	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – Ledger	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – Invoices	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**

BM	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – Bank statements	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
BM	School Fund – School Journey books	No		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
BM	Student Grant Applications	Yes		Current year + 6 years then review	SECURE DISPOSAL	**IL2–PROTECT**
BM	Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
BM	Petty cash books	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

9 Property						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
BM	Title Deeds	No		Permanent	Permanent -these should follow the property unless the property has been registered at the Land Registry	**IL2–PROTECT**
BM	Plans	No		Permanent	Retain in school whilst operational	**IL3 - RESTRICTED**
BM	Maintenance and contractors	No	Financial Regulations	Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Leases	No		Expiry of lease + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Lettings	No		Current year + 3 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**
BM	Maintenance log books	No		Last entry + 10 years	SECURE DISPOSAL	**IL1–Unclassified**
BM	Contractors' Reports	No		Current year + 6 years	SECURE DISPOSAL	**IL2–PROTECT**

10 Department for Children, Schools and Families						
IAO	**Basic file description**	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Protective Marking Classification**
CtG	OFSTED reports and papers	No		Replace former report with any new inspection report	Schools may wish to retain copies of former reports for longer	**IL2–PROTECT**
DM	Returns	No		Current year + 6 years	SECURE DISPOSAL	**IL3 - RESTRICTED**
HT/ CtG	Circulars from Department for Children, Schools and Families	No		Whilst operationally required	Review to see whether a further retention period is required	**IL1–Unclassified**

Appendix 2
INCIDENT SECURITY REPORT

ISIR Reference	ISIR (year)(no) e.g. ISIR 2017 001	Date opened:	
Short Title			
Associated Reference Number:		ISIR owner (provide name and job title):	
Police Crime No:		Device ID:	
Lost Y/N	Stolen Y/N	Other	
Impact Risk Low Medium High			
Has insurance been informed? Yes/No Date:			
Description of Data lost (Format, Volume, Personal Dara, from which system):			
Has the data/system owner been informed? Yes/No Date: Name:			
Definition of the Problem and how it was reported, including history of events:			
Impact Summary			
Detail of resolution			
Root Cause Analysis			
Corrective Actions:			

Ref:	Action	Target date	Owner	Complete?

Lessons Learned:	
Ref	Lesson Learned

Date agreed for Evaluation		Evaluation Date	
Date Closed		Head teacher Signoff	

Appendix 3
Subject Access Request Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide **proof of your identity.** Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of two documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Administration Fee

We do not generally charge for Subject Access Requests.

Section 1

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title:
Surname/Family Name:
First Name(s)/Forenames:
Date of Birth:
Address: **Postcode:**
Previous Addresses: **Post Code:**
Day Time Telephone Number

I am enclosing copies as proof of identity: Birth Certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐
Personal Information If you want to know what information is held in specific records please indicate in the box below. Please tell us if you know in what capacity the information is held, together with any names or dates you have.
Details:

Employment records If you are now, or have been employed by Turton school and are seeking personal information in relation to your employment please provide details of your staff number/dates of employment.

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title
Surname/Family Name:
First Name(s)/Forenames:
Date of Birth:
Address: Postcode:
Day Time Telephone Number:

I am enclosing copies as proof of identity: Birth Certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐
What is your relationship to the data subject? (e.g. parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject: Letter of authority ☐ Lasting or Enduring Power of Attorney ☐ Evidence of parental responsibility ☐ Other (give details):

Data Subject declaration: I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Turton school is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.	
Name:	
Signature:	Date:

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

I wish to:

Receive the information in electronic form * ☐

Receive the information by post ** ☐

Collect the information in person ☐

View a copy of the information only ☐

Go through the information with a member of staff ☐

* Some files may be too large to transmit electronically and we may have to supply in CD format)
** Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity to:

Head Teacher

Turton School

Bromley cross Road

Bolton

BL7 9LT

info@Turton.uk.com

Appendix 4

Request for Personal Data Form

To

Details of applicant

Name of applicant	
Job title	
Department and Section	
Full Address	
Telephone number	
e-mail address or fax number	
Investigation reference / Operation Name	
Date	

Details of application

1. This request is made pursuant to the Law Enforcement Directive. I can confirm that this request complies with the following non-disclosure provisions

Section 29

☐ The data is necessary for the prevention or detection of crime

☐ The data is necessary for the apprehension or prosecution of offenders

---

Section 35

☐ The data is necessary for the purpose of or in connection with present legal Proceedings

☐ The data is necessary for the purpose of or in connection with prospective legal proceedings

2. I require the following information

3. Why I require the information

4. What statutory powers does the requester have to demand the information
5. **I can confirm that the information you provide will be held in the strictest confidence and will not be further processed beyond the purpose for which it was requested.** **I have grounds believing that failure to disclose the required information will be likely to prejudice my enquiries and can confirm that the details supplied on this form are, to the best of my knowledge, correct.** **I am aware of the provisions of Law Enforcement Directive, regarding the unlawful obtaining of personal details.**
Signature Print Name

Appendix 5 - Procedures for identifying and reporting of data breaches