Data Protection (GDPR) Policy

History of document: To be reviewed annually and re-approved every two years, or sooner if deemed necessary.

Issue	Author	Date written	Board Approval	Comments
1	C Burt	10-10-17	17-10-17	
2	C Burt	23-2-18	22-05-18	GDPR Version
3	J Goodwin	16-7-20	21-07-20	General updates/formatting Addition of SAR form

Contents

1. Aims

Yorkshire Causeway Schools Trust (YCST) aims to ensure that all personal data collected about employees, pupils, parents/carers, governors, visitors and other individuals who come into contact with them is collected, stored and processed in accordance with the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data regardless of whether it is held in paper files or electronically.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with the Trust's Funding Agreement and Articles of Association.

Trust schools also have a duty to issue a Privacy Notice to pupils/parents/carers/staff which summarises the information held, why it is held and the other parties to whom it may be passed on.

All staff involved with the collection, processing and disclosure of personal information will be aware of their duties and responsibilities within these guidelines.

General information about the GDPR can be obtained from the Office of the Information Commissioner (website http://www.ico.gov.uk).

3. Definitions

Personal data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including: • name • identification number • location data • online identifier reflecting changes in technology and the way organisations collect information about people. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. The GDPR is applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
Sensitive personal data (special categories of personal data – GDPR, article 9)	Personal data which is more sensitive and so requires greater protection. This includes: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data for the purpose of uniquely identifying a natural person (eg fingerprints, retina and iris patterns), • health – physical or mental

	• sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see GDPR, article 10).
Processing	Any action involving personal information, including obtaining, viewing, recording, copying, amending, adding, deleting, extracting, storing, disclosing, destroying or otherwise using information. Processing can be automated or manual.
Data subject	The identified or identifiable individual who is the subject of personal data or the person to whom the information relates
Data controller	A person or organisation that determines the purposes and the means of processing personal data
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Parent	Has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child
Personal data breach	A breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

4. The data controller

The Trust is the Data Controller under the GDPR and will endeavour to ensure that all personal information is processed in compliance with this Policy and the principles of the GDPR. The Trust, on behalf of its schools, has a duty to be registered as Data Controller with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on the ICO's website.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

The Board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The Trust's DPO is contactable via the Headteacher in the first instance.

5.3 Headteachers

The Trust's headteachers act as the representatives of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing the school of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - if there has been a data breach
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

Under GDPR the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data

may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The Trust is committed to maintaining these principles at all times. This means we will:

- tell you the lawful basis for processing information when we collect it
- tell you what purposes we will use information for when we collect it
- if information will be shared we will tell you why, with whom and under what circumstances
- check the quality and accuracy of the information we hold to ensure it is current, adequate, relevant and necessary
- apply our records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system
- share personal information with others only when it is necessary and legally appropriate to do so and set out clear procedures for responding to requests for access to personal information, known as subject access requests
- train our staff so that they are aware of our policies and procedures
- update this policy, as necessary, to reflect best practice or amendments made to the GDPR.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- the data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- the data needs to be processed so that the school can **comply with a legal obligation**
- the data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- the data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- the data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

- the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Records Management Policy and Records Retention Schedule.

The Trust will aim to ensure data held about pupils, parents/carers and staff is as accurate and up to date as reasonably possible. The Trust requests all data subjects to inform us of any changes to information held, and offers frequent reminders to data subjects to do this. Additionally, data record sheets for pupils are reviewed annually and parents/carers are asked to update and check the data collection sheets.

The Trust will only gather and process data that it considers necessary to carry out its educational purposes effectively. It will ensure that data is not held any longer than is necessary and, once no longer needed, it is properly destroyed/erased.

8. Sharing personal data – authorised disclosures

The Trust will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Trust will need to disclose data without explicit consent for that occasion. This is covered by the GDPR (Regulation (EU) 2016/679), Article 6 (1) (e), 'public task'.

These circumstances are largely but not exclusively limited to:-

- pupil data disclosed to authorised recipients, related to education and administration, necessary for the Trust to perform its statutory duties and obligations.

- pupil data disclosed to parents/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- where there is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters, such as HMRC.
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form agreeing not to disclose the data outside the school. Such persons are contractually bound not to disclose personal data.
- the prevention or detection of a crime and/or fraud or the apprehension or prosecution of offenders.
- to satisfy our safeguarding obligations.

Only authorised staff are allowed to make external disclosures of personal data. Data used within the Trust by administrative staff, teachers and other officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information in order to do their work.

The Trust will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

9. Processing personal data

Personal data (including sensitive personal data, where appropriate) is processed by the Trust strictly in accordance with the General Data Protection Regulation (GDPR) in order to:

- Support pupils' teaching and learning
- Safeguard all pupils in our care
- Provide appropriate pastoral care
- Monitor and report on pupil progress
- Comply with law regarding data sharing
- Publish examination results
- Assess the quality of our services
- Assess how individual schools, and the Trust as a whole, is performing
- Communicate with former pupils
- Monitor pupils' official Email communications and internet use etc. for the purpose of ensuring compliance with the Trust's ICT Acceptable Use Policy
- Where appropriate, promote the Trust to prospective pupils

10. Individual Rights

The GDPR provides the following rights for individuals and the Trust is committed to maintaining these principles at all times:

1. The right to be **informed** - we will provide 'fair processing information', typically through a privacy notice.
2. The right of **access** – we will allow individuals to access their personal data so that they are aware of and can verify the lawfulness of the processing
3. The right to **rectification** – we will ensure individuals entitlement to have personal data rectified if it is inaccurate or incomplete.
4. The right to **erasure** – we will meet the broad principle underpinning this right, of enabling an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances.
5. The right to **restrict processing -** in specific circumstances, permit individuals to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.
6. The right to **data portability** – we will allow individuals to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies:
   - to personal data an individual has provided to a controller;
   - where the processing is based on the individual's consent or for the performance of a contract; and
   - when processing is carried out by automated means.
7. The right to **object** – we will permit individuals to object on "grounds relating to his or her particular situation". We will stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or the processing is for the establishment, exercise or defence of legal claims.
8. Rights in relation to **automated decision making and profiling** – we will identify whether any of our processing falls under Article 22 "Automated individual decision-making, including profiling" and, if so, make sure that we give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that your systems are working as intended.

11. Subject Access Requests and other rights of individuals

Individuals have the right to access their personal data that the Trust holds about them.

The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals have the right to obtain:

- confirmation that their personal data is being processed
- access to a copy of their personal data
- the purposes of the data processing
- the categories of personal data concerned

- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible the criteria used to determine this period
- where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- the right to lodge a complaint with the ICO or another supervisory authority
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- the safeguards provided if the data is being transferred internationally.
- other supplementary information – this largely corresponds to the information that is provided in a privacy notice.

Requests for information will ideally be made in writing (including email) on the attached form, and be addressed to the Headteacher, to include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested

If the initial request does not clearly identify the information required, then further enquiries will be made.

If staff receive a subject access request in any form then they must immediately forward it to the Headteacher. The Headteacher will correspondingly notify the DPO.

11.1 Children and subject access requests

Personal data about a child belongs to that child, and not their parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Pupils have a right of access under the GDPR to their own information.

The determination of whether a child can act for themselves is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request.

For any parent/carer request regarding a pupil the Headteacher may discuss the request with the pupil and take their views into account when making a decision. A pupil with competency to understand can refuse to consent to the request for their records. Where the pupil is not deemed to be competent to act for themselves in this regard, a parent or carer may make the decision on behalf of the pupil.

11.2 Responding to subject access requests

11.2.1 Any individual has the right of access to information held about them. The identity of the requestor must be established before the disclosure of any personal information,

and it may be necessary to undertake checks regarding proof of relationship to the pupil. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- birth / marriage certificate
- P45/P60
- credit card or mortgage statement

This list is not exhaustive.

11.2.2 The Trust may make a charge for the provision of information, dependent upon the following extracts from the GDPR:

- you must provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive
- you may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests
- the fee must be based on the administrative cost of providing the information.

11.2.3 Information must be provided without delay and at the latest within **one month** of receipt. However, this month will not commence until after receipt of fees or clarification of information sought.

11.2.4 We will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

11.2.5 Where we process a large quantity of information about an individual, the GDPR permit us to ask individuals to specify the information the request relates to (Recital 63) and although the GDPR does not include an exemption for requests that relate to large amounts of data, we are able to consider whether the request is manifestly unfounded or excessive.

11.2.6 Third party information is that which has been provided by another, such as the Police, local authority, health care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the one month statutory timescale.

11.2.7 We may not disclose information for a variety of reasons, such as if it:

- may cause serious harm to the physical or mental health or emotional condition of the individual, or another
- would reveal that the pupil is being, or has been abused or is at risk of abuse where disclosure of that information would not be in the pupil's best interests

- would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

11.2.8 Should we refuse to respond to a request, we will explain to the individual why, informing them of their right to complain to the ICO or they can seek to enforce their subject access through the courts.

11.2.9 If there are concerns over the disclosure of information then additional advice may be sought.

11.2.10 Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11.2.11 Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped. If the request is made electronically, you should provide the information in a commonly used electronic format.

11.2.12 Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used. If information is shared electronically then this should be in a commonly used electronic format and by secure means.

11.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances

- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the education record

The right of those entitled to have access to curricular and educational records as defined within The School Information (England) Regulations 2008. Legally, this provision applies only to maintained schools. However, the Trust will consider any request for such records on a case by case basis. The process set out in this Policy relates solely to subject access requests made under the GDPR.

13. CCTV

The Trust uses CCTV in various locations around its school sites to support its safeguarding and pupil safety responsibilities and to protect the security of its sites. We will adhere to the ICO's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

14. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- within school on notice boards and in school magazines, brochures, newsletters, etc.
- within school for the identification of children with specific medical issues/allergies etc. to assist with our safeguarding and medical responsibilities.
- outside of school by external agencies such as the school photographer, newspapers, campaigns
- online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Any photographs and videos taken by parent/s carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all relevant parents/carers have agreed to this.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - for all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. Data Security

The Trust undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed).

Physical Security:

- Appropriate building security measures are in place, such as key fob entry, alarms, window bars, deadlocks.

- Only authorised persons are allowed access to servers which are secured within each location.
- Disks, tapes and printouts are locked away securely when not in use.
- Visitors to schools are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.
- Security software is installed on all computers containing personal data.
- Only authorised users are allowed access to the computer files and password changes are regularly undertaken.
- Computer files are backed up regularly.

Procedural Security:
- In order to be given authorised access to the computer network, staff will have to undergo checks and will sign an Acceptable Use Agreement.
- All staff are trained in their data protection obligations and their knowledge updated as necessary.
- Computer printouts as well as source documents are shredded before disposal.
- Staff are aware they should 'lock' or close down computers when not in use.
- Deliberate data protection breaches are treated very seriously. Staff are aware that such breaches are a disciplinary matter and could lead to dismissal.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible. Our procedure is outlined in Appendix 1.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.

We will ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

Such breaches in a school context may include, but are not limited to:

- a non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- safeguarding information being made available to an unauthorised person
- the theft of a school laptop containing non-encrypted personal data about pupils.

19. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years for approval by with the Trust Board.

21. Complaints

Complaints regarding these procedures, or any other data protection matter, should be made in line with the Trust's Complaints Policy. Complaints that involve consideration of personal data or sensitive personal data may be referred to the Information Commissioner.

22. Links with other Trust policies

- Privacy notice – pupils / staff
- Freedom of Information Publication Scheme / Charging Policy
- CCTV Policy
- Computer Network and ICT Acceptable Use Agreement (for Students/Adults/Visitors)
- Records Management Policy
- Document Retention Schedule

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - lost
  - stolen
  - destroyed
  - altered
  - disclosed or made available where it should not have been
  - made available to unauthorised people.
- The DPO will alert the appropriate headteacher and the chair of governors in the first instance, and the Trust Board if appropriate.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - loss of control over their data
  - discrimination
  - identify theft or fraud
  - financial loss
  - unauthorised reversal of pseudonymisation (for example, key-coding)
  - damage to reputation
  - loss of confidentiality
  - any other significant economic or social disadvantage to the individual(s) concerned.

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are retained by the Trust.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned

- the categories and approximate number of personal data records concerned
- the name and contact details of the DPO
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - the name and contact details of the DPO
  - a description of the likely consequences of the personal data breach
  - a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - facts and cause
  - effects
  - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be retained by the Trust.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the appropriate actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. An example of such an action following a breach is:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach that might require action could include:

- details of pupil premium interventions for named children being published on the school website
- non-anonymised pupil exam results or staff pay information being shared with governors
- a school laptop containing non-encrypted sensitive personal data being stolen or hacked
- the school's cashless payment provider being hacked and parents' financial details stolen.

Personal Data Subject Access Request

If you wish to make a request for personal data under data protection legislation, it will help us to respond to your request as quickly as possible if you could please complete this form. In most cases we will respond to your request within one calendar month although we may extend this time if the request is complex. If this is necessary we will inform you as such within one month of receipt of the request, together with the reason(s) for the delay.

Your name				
Phone number: (optional – used to contact you about your request)			E-mail / postal address: (your preferred contact method)	
Are you the data subject?	Yes ☐	No ☐	Your relationship to the Data Subject, or state "not applicable"	
If you selected "no", please give the name of the Data Subject:				
If you are requesting data on behalf of a pupil, we will require consent from the pupil if we believe that they have the capacity to understand this request (normally 13 years or over).				
Do you want a copy of some personal data?	Yes ☐	No ☐		
If No, please select another option below:				

Information about processing	☐	Correction of data	☐	Erasure of data	☐	Objection to/restrict use of data	☐

If Yes, what data? Please describe below and provide as much detail as possible to aid us in our search
I confirm that the information provided above is accurate and true, that I may be contacted to confirm my identity and that it may be necessary to obtain more detailed information in order to locate the correct information sought.

Signed:		Date:	

Please return this form to the School Office for the attention of the Headteacher [July 2020]

OFFICE USE ONLY	Date
Request received	
Request acknowledged	
Fee notice issued or N/A	
Fee received	
Completed	