Brownhill
LEARNING COMMUNITY

DATA PROTECTION POLICY

APPROVED BY	**AWAITING APPOVAL**
LAST REVIEWED ON	**SEPTEMBER 2021**
NEXT REVIEW DUE BY	**SEPTEMBER 2022**
BROWNHILL LEARNING COMMUNITY IS RESPONSIBLE FOR MONITORING AND REVIEWING THIS POLICY	

Contents…

1. Aims…

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance…

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. Parents, or those with parental responsibility, have a legal right to free access to their child's education record (which includes most information about a pupil) within 15 school days of receipt of a written request.

3. Definitions…

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller…

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities…

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

5.1 Governing board…

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Manager & Data Protection Officer…

The Data Manager at Brownhill Learning Community is responsible for overseeing the implementation of this policy, monitoring our compliance with UK data protection law, develop related policies and guidelines where applicable and ensure staff have appropriate training.

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

The Data Manager is also the first point of contact for individuals whose data the school processes, and for the ICO. Please contact the Data Manager by emailing office@theblc.org.uk or telephoning 0300 303 8384.

If you have a concern about the schools data protection practice you can contact our Data Protection Officer - DPOSchools@Rochdale.Gov.UK.

5.3 Headteacher

The Headteacher acts as the representative 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 Data Manager in the following circumstances:

- With any questions about the operation of this policy, UK 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 UK
- 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…

The UK GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

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 UK 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (when the processing is not for any tasks the school perms as a public authority) 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 under UK data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under UK data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

  - ❖ Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
  - ❖ Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - ❖ Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals…

For our full Policy please refer to our 'GDPR Individual Rights' Procedure at www.theblc.org.uk or request one via the School Office.

9.1 Subject access requests…

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

Personal data about a child belongs to that child, and not the child's 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.

9.2 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 (see section 7), 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 (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
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 Data Manager or DPO. If staff receive such a request, they must immediately forward it to the Data Manager.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. 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.

Any enquiries about the CCTV system should be directed to the ICT Network Manager at Brownhill Learning Community.

12. 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, or Social Workers for a looked after child, for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/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 the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- 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.

Photographs/videos which form evidence for an award are permitted to be taken without consent.

13. Mobile Phones

Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.

Staff will not take pictures or recordings of pupils on their personal phones or cameras or store any personal data about them.

Pupils will hand in their mobile phones/other devices at the beginning of the School day and returned at the end of their School day.

Staff who have a work mobile phone must ensure this is kept in a secure place when not in use and must not be left in an unattended vehicle.

14. 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 Data Protection Officer and School Data Manager, 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 UK data protection law (see section 6)
- Completing data protection 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 Data Manager 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 UK 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 UK, where different data protection laws may 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, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Staff will not store personal data on pen drives.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Access to offices/rooms where there is a significant amount of confidential personal data (eg. admin office, SLT/SMT offices) should be limited to staff and authorised visitors – Pupils and Parents should not be allowed in these rooms.
- Lock your computer when not in use – Control, Alt, Delete, Lock or Windows Key and L – this ensures there is no unauthorised access by pupils or other persons.
- Individual Pupil Files...

  Individual Pupil Files (pink) are kept securely in each Site's Admin Office. For Home Tuition the files are kept by the Home Tuition Co-ordinator in her office.

  If a member of Staff needs to take a file(s) out of the office – a record of this must be completed. Staff should fill in the Pupil File Location Log held in each Admin/Home Tuition Office completing: Date, Time, Pupil Name(s), Staff Name, where is the file being taken to, Return Date & Time and add any Comments if necessary.

  If pupil files are being transferred from one Site to another (eg. a pupil has moved sites) then the pupil file must be signed out of one site and signed into the other.

  Pupils may also move to/from Home Tuition, therefore Pupil files should also be signed in/out the Admin Office/Home Tuition.

  Pupil files must not be passed from member of Staff to another – files must be signed out of the office by the member of Staff using it and then signed back in. If another member of Staff needs access to it they should sign the file out themselves.
- When taking personal data off site – laptops and papers should be carried in separate bags
- If taking paper copies of eg. pupil address/telephone numbers off site this must be printed just prior to leaving the site and must be shredded immediately after the information is finished with
- Anything which contains personal data must not be left unattended in a car – the staff members should take it with them at all times
- Staff are asked to use strong passwords to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Passwords should not be stored in an unsecure location – lock away or use Onenote. Passwords for laptops should not be kept in the laptop bag.
- Encryption software is used to protect all portable devices and removable media.
- Staff, pupils or governors are instructed not to store personal data on their own devices

- Staff can access personal data on their own devices, eg. either email or Sharepoint (via Remote Access) – but they must sign in and then out of www.theblc.org.uk to ensure access is secure
- Staff and Governors must not add work email to their personal Mail Boxes
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
- Any emails containing personal data being sent to an outside person/agency should be encrypted. Create your email and on the subject line type the word – encrypt – followed by your subject.
- Staff and Governors can send emails containing personal data to Rochdale Authority by using a secure egress switch account.

The School recognises that there are risks associated with managing records in order to meet legislative requirements. Non-compliance with this policy could have a significant effect on the efficient operation of the school and may result in financial loss and an inability to provide necessary services and information to customers. This policy is intended to mitigate those risks.

16. 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK data protection law. Refer to our Retention Schedule within the 'irms Toolkit for Schools'

NB: Section 3.2. Secondary Pupils' Education Record/Child Protection Information states the retention period of Date of Birth + 25 Years but under Section 3.4 Pupils who have EHC plans should have an additional 6 Years. The BLC will keep all Pupil records (regardless of whether they have an EHC) for Date of Birth + 31 Years.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. 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

As part of the GDPR training the Data Manager has conveyed the message from the Headteacher and SLT that anybody responsible for a personal data breach may receive some form of sanction.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Sections 170-173 of the Data Protection Act 2018 cover offences under the Act which include obtaining, disclosing or retaining personal data without the consent of the data controller. Examples could include: misusing School systems to source information for personal use, 'hacking' of School systems, selling personal data held on the School system.

18. 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 school's processes make it necessary.

19. Monitoring arrangements

This policy will be subject to compliance audits instigated and overseen by the School's Data Manager.

Information Governance is viewed seriously by the School. Any breach of this Policy and other associated requirements, will be considered and investigated under both the Schools Disciplinary Procedure and Information Security Breach Procedure or restricted to one of the two procedures. Dependent upon the seriousness of the allegations and outcome of investigations, and employees should be aware that this may result in disciplinary action an outcome of which may have serious consequences for an employee's continued employment.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Sections 170 – 173 of the Data Protection Act 2018 cover offences under the Act which include obtaining, disclosing or retaining personal data without the consent of the data controller. Examples could include: misusing council systems to source information for personal use, 'hacking' of council systems, selling personal data held on a Council system.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Retention Schedule
- CCTV
- Individual Rights
- Acceptable Use of ICT
- Safeguarding

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 Data Manager at Brownhill Learning Community

- The Data Manager will investigate the report, and determine whether a breach has occurred. To decide, the Data Manager 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

- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

- If a breach has occurred or it is considered to be likely that is the case the Data Manager will alert the headteacher and the chair of governors

- The Data Manager will contact the Data Protection Officer for advice if needed

- The Data Manager 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 Data Protection Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The Data Protection Officer 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 Data Protection Officer 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 Data Protection Officer must notify the ICO.

- The Data Manager 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 stored on Sharepoint.

- Where the ICO must be notified, the Data Protection Officer will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Data Protection Officer 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 Data Manager and Data Protection Officer

    - 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 Data Protection Officer 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 Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible

- The Data Protection Officer 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 Data Protection Officer 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 Data Protection Officer
    - 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 Data Protection Officer 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 Data Manager 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 stored on Sharepoint.

- An initial internal investigation will take place by the Data Manager to review what has happened and how it can be stopped from happening again. An Internal Investigation Data Breach form will be completed the Investigating Officer will report their findings to the Headteacher and Chair of Governors who will consider what internal sanction is appropriate, eg. Additional training, disciplinary procedure. If necessary, further advice would be sought from the Authority's Personnel Department.

- If further investigation is needed after the Data Manager's report these are the Staff roles…

INVESTIGATING OFFICER	MEMBER OF STAFF REPONSIBLE FOR BREACH
Chair of Governors	Headteacher
Headteacher	Member of Senior Leadership Team
Member of Senior Leadership Team	Member of Senior Management Team
Member of Senior Management Team	Any other Member of Staff

Actions to minimise the impact of data breaches

We will take the actions set out below 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.

If a member of Staff loses/has stolen any work equipment (eg. laptop/mobile phone) an estimated cost of the lost items will be gathered and the member of Staff will be asked to contribute to the replacement cost.

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 Data Manager as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Manager will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Data Manager 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 Data Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Manager 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
- If safeguarding information is compromised the Data Manager will inform the Designated Safeguarding Lead.

Other types of breach 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
- Hardcopy reports sent to the wrong pupils or families.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Sections 170-173 of the Data Protection Act 2018 cover offences under the Act which include obtaining, disclosing or retaining personal data without the consent of the data controller. Examples could include: misusing School systems to source information for personal use, 'hacking' of School systems, selling personal data held on the School system.