CARDIFF SIXTH FORM COLLEGE

Dukes EDUCATION

Data Protection Policy

August 2025

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
Version 1	Charlotte McQuaid	November 2018	Gareth Collier	January 2019

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
January 2019	Document Formatting	Cerys Williamson	October 2019	Gareth Collier	October 2019
October 2019	Annual Review	Charlotte McQuaid	August 2020	Gareth Collier	August 2020
August 2020	Annual Review	Charlotte McQuaid	August 2021	Gareth Collier	August 2021
August 2021	Annual Review	Charlotte McQuaid	November 2022	Gareth Collier	November 2022
November 2022	Annual Review	Charlotte McQuaid	August 2023	Tom Arrand	September 2023
August 2024	Annual Review	Charlotte McQuaid	August 2024	Rob Humphreys	August 2025

Contents

Policy

1.0 Aims

1.1 Cardiff Sixth Form College 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 the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2.0 Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the expected provisions of 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.

2.2 Biometric data is a general term used to refer to any computer data that is created during a biometric process. This includes samples, models, fingerprints, similarity scores and all verification or identification data excluding the individual's name and demographics.

2.3 CSFC meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.4 Identifiable imagery (CCTV) is considered as personal data under the GDPR and therefore, at a data protection level, requires the same level of thought and care that is being paid to other affected areas of the business.

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

3.0 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 Includes IP addresses and cookie identifiers which may be personal data.

	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.

4.0 The Data Controller

4.1 Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

4.2 The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.0 Roles and responsibilities

5.1 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.

5.2 Governing board

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

5.3 Data protection champion

5.3.1 The data protection champion is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.3.2 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.

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

5.3.4 Full details of the GDPR Champion's responsibilities are set out in their job description.

5.3.5 Our GDPR Champion [Academic & Data Manager] is contactable via [data.protection@ccoex.com].

5.4 Principal

5.4.1 The Principal acts as the representative of the data controller on a day-to-day basis.

5.5 All staff

5.5.1 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 GDPR Champion 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

6.0 Data protection principles

6.1 The GDPR is based on data protection principles that our school must comply with.

6.2 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.

7.0 Collecting personal data

7.1 <u>Lawfulness, fairness and transparency</u>

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

7.1.2 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

7.1.3 The data needs to be processed so that the school can comply with a legal obligation

7.1.4 The data needs to be processed to ensure the vital interests of the individual e.g., to protect someone's life

7.1.5 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

7.1.6 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)

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

7.1.8 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.

7.2 Limitation, minimisation and accuracy

7.2.1 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.

7.2.2 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.

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

7.2.4 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 Retention Policy.

8.0 Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

8.2 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 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

8.3 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

8.4 Pupil data will be shared freely on a strict need to know basis with relevant staff and or external professionals if a student is deemed at risk due to safeguarding incidents and or if there is a medical concern. Please refer to the Safeguarding and Child Protection Policy and Health &

Medical policy for further details. In these instances, permission to share information may not be sought.

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

8.6 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9.0 Subject access requests and other rights of individuals

9.1 Subject access requests (SAR)

9.1.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. SAR requests can be made verbally or in writing, including by social media. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the 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
- 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

9.1.2 SARs should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

9.1.3 If staff receive a SAR, they must immediately forward it to the GDPR Champion.

9.1.4 <u>Children and subject access requests</u>

9.1.4.1 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 SAR 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.

9.1.4.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at our school may be granted without the express

permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.1.4.3 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.1.5 Responding to subject access requests

9.1.5.1 When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

9.1.5.2 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

9.1.5.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs.

9.1.5.4 A request will be deemed unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.1.5.5 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.2 Other data protection rights of the individual

9.2.1 In addition to the right to make a SAR (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals 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
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to 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)

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

10.0 Parental requests to see the educational record

10.1 As for all independent schools: there is no automatic parental right of access to the educational record.

11.0 CCTV

11.1 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.

11.2 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.

11.3 Any enquiries about the CCTV system should be directed to the College Service Manager.

12.0 Photographs and videos

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

12.2 We will obtain written consent from students for photographs and videos to be taken of them for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the student.

12.3 Uses may include, but are not limited to:

- 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

12.4 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.

12.5 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.

13.0 Data protection by design and default

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

13.1.1 Appointing a suitably qualified GDPR Champion, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

13.1.2 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 (see section 6)

13.1.3 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 GDPR Champion will advise on this process)

13.1.4 Integrating data protection into internal documents including this policy, any related policies and privacy notices

13.1.5 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

13.1.6 Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

13.1.7 Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and GDPR Champion 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, 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

14.0 Data security and storage of records

14.1 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
- 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

- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. Please see our IT Acceptable Use Policy for further information.

14.2 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 (see section 8)

15.0 Data Retention

15.1 In accordance with the Data Protection Act 2018 (General Data Protection Regulation) and good practice advice from the National Independent Bursars Association. The table below provides minimum retention periods for all data held or managed by the college, some of which may be personal data.

Data Area	Record	Retention Period
COLLEGE-SPECIFIC RECORDS	Registration documents of College	Permanent
	Attendance Register	6 years from last date of entry, then archive.
	Minutes of Governors' meetings	6 years from date of meeting
	Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g., marks / timetables / assignments)
INDIVIDUAL STUDENT RECORDS	Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if student not admitted, no longer than 1 year from that decision).

	Examination results (external or internal)	6 years from student leaving college
	Student file including: • Student reports • Student performance records • Student medical records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the student).
	Special educational needs records (to be risk assessed individually)	35 years from Date of birth (allowing for special extensions to statutory limitation period)
SAFEGUARDING	Policies and procedures (including audits)	Keep a permanent record of historic policies
	DBS disclosure certificates (if held)	12 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
	Accident / Incident reporting	Indefinitely (as recommend by the Goddard inquiry)
	Child Protection files	Indefinitely (as recommend by the Goddard inquiry)
EMPLOYEE / PERSONNEL RECORDS	Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
	Contracts of employment/contract for	7 years from effective date of end of contract

	services/consultancy agreements (self-employed or contracted personal) (offer letters and variation letters)	
	Employee appraisals or reviews	Duration of employment plus 7 years
	Staff personnel file (Includes grievances, capability and disciplinary documentation, qualifications, termination documentation, references, training records, parental leave records)	As above, but do not delete any information which may be relevant to historic safeguarding claims.
	Payroll, salary, maternity pay records	6 years
	Pension or other benefit schedule records	Permanent, depending on nature of scheme
	Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
	Immigration records	4 years
	Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS	Insurance policy certificates (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
ENVIRONMENTAL, HEALTH & DATA	Accidents to children	25 years from birth (longer for safeguarding – see safeguarding)

	Accident at work records (staff)	4 years from date of accident, but review case-by-case where possible
	Staff use of hazardous substances	7 years from end of date of use
	Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.
	Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)

16.0 Disposal of records

16.1 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.

16.2 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 data protection law.

17.0 Personal data breaches

17.1 The school will make all reasonable endeavours to ensure that there are no personal data breaches.

17.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

17.3 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

18.0 Training

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

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

19.0 Monitoring arrangements

19.1 The GDPR Champion is responsible for monitoring and reviewing this policy.

19.2 This policy will be reviewed and updated, if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

19.3 Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.

20.0 Links with other policies

20.1 This data protection policy is linked to our:

- Acceptable Use policy
- Health & Safety Policy
- Health and Medical Policy

Appendix 1

Personal data breach procedure

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

1.1 On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the GDPR Champion.

1.2 The GDPR Champion will investigate the report and determine whether a breach has occurred. To decide, the GDPR Champion 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

1.3 The GDPR Champion will alert the Principal, the chair of governors and the central GDPR team.

1.4 The GDPR Champion will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors, and with support from the central GDPR team, where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

1.5 The GDPR Champion will assess the potential consequences, based on how serious they are, and how likely they are to happen

1.6 The GDPR Champion 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 GDPR Champion 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

1.7 If it is likely that there will be a risk to people's rights and freedoms, the GDPR Champion must notify the ICO.

1.8 The GDPR Champion 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 securely on the online storage site provided by our Solicitor Bird and Bird who we consult with in matter data protection)

1.9 Where the ICO must be notified, the GDPR Champion will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the GDPR Champion will set out:

1.10 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 GDPR Champion
- 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

1.11 If all the above details are not yet known, the GDPR Champion 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 GDPR Champion expects to have further information. The GDPR Champion will submit the remaining information as soon as possible

1.12 The GDPR Champion 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 GDPR Champion 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 GDPR Champion
- 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

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

1.14 The GDPR Champion 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 securely locally on the Data Breach Log.

1.15 The GDPR Champion and Principal 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

1.0 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. For example:

- 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 GDPR Champion as soon as they become aware of the error

1.1 If the sender is unavailable or cannot recall the email for any reason, the GDPR Champion will ask the ICT department to recall it

1.2 In any cases where the recall is unsuccessful, the GDPR Champion 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

1.3 The GDPR Champion will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

1.4 The GDPR Champion 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

1.5 Other types of breach that you might want to consider 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