Policy Reference G03
Data Protection (GDPR) Policy

Every school within Cumbria Futures Federation aims to provide a safe and hardworking environment where every child can be successful, whatever their abilities.

Our Values

- Courage and Compassion
- Inclusion and Equality
- Respect and Courtesy
- Optimism and Perseverance
- Forgiveness and Tolerance
- Ambition and Achievement

Version No	Author/Owner	Date Written	Note of amendments made	Authorised by	Date
01-2018	JR	August 2018	New policy created from previous GDPR Policy	Governors	11/09/2018
01-2020	JR	October 2020	Reviewed, Covid-19 information added	Governors	

Contents

1. Aims

Our Federation aims to ensure that all personal data collected about staff, students, 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.

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

Schools are required to keep and process certain information about its students, staff and other individuals for various purposes such as:

- To support student learning;
- To monitor and report on student progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To ensure we operate efficiently and effectively;
- To recruit and pay staff;
- To collect fees;
- To comply with legal obligations to funding bodies and the government;
- To enable financial modelling and planning;
- To develop a comprehensive picture of the workforce and how it is deployed.

1.3 Schools within our Federation may be required to share personal information about its students or staff with other schools, organisations, the LA and social services.

1.4 This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage and audio and video systems.

Given current (Autumn 2020) circumstances, a Covid Addendum has been added to the Federation's data protection overview and has been published via notices and on our websites:

Data Privacy Notice

For the attention of parents, visitors, students and staff:

Personal data of students, employees, parents or visitors to school may be shared with NHS / Public Health Agencies / NHS Track and Trace where relevant to the Covid pandemic.

We will share information only with appropriate authorities, only through secure methods and we will limit the data shared to the minimum necessary. We will verify the identity of individuals requesting personal data and keep a record of the data shared, and where practical will notify individuals whose data has been shared.

If you have any concerns or queries please contact our Data Protection Lead via the School Office.

2. Legislation and guidance

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.

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 (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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. This might include: • Employees (current and former), • Students (including former students), • Recruitment applicants (successful and unsuccessful), • Agency workers (current and former), • Casual workers (current and former), • Contract workers (current and former), • Volunteers (including members, directors and governors) and those on work placements, • Claimants.
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 Federation processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.
Each school within our Federation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.
The Federation itself does not process any personal data, all processing activities take place within the individual schools within the Federation.

5. Roles and responsibilities

This policy applies to **all staff** employed by the schools within our Federation, and to external organisations or individuals working on our behalf including Governors. Individuals who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that all schools within our Federation comply 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 governing board and, where relevant, report to the board their advice and recommendations on any data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Dale Stephenson and is contactable at Netherhall School on 01900 813434.

5.3 Data protection lead (DPL)

Because our DPO is located offsite, for day-to-day matters that don't involve breaches our Data Protection Lead (DPL) will deal with concerns and queries and with internal procedural issues. Our DPL is Jennifer Rowlands.

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 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

The GDPR is based on data protection principles that our Federation 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 Federation 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 data protection law:

- The data needs to be processed so that the Federation or schools within the Federation can **fulfil a contract** with the individual, or the individual has asked us to take specific steps before entering into a contract
- The data needs to be processed so that we 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 we, 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 Federation or school within the Federation, 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 student) 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.
Where we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 16 (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 Information and Records Management Society's toolkit for schools and relevant modifications required by Cumbria County Council.

8. Sharing personal data

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

- There is an issue with a student 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 students – 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

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

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 students or staff.
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. Consent

It is not always necessary to gain consent before processing personal data but when it is, consent must be a positive indication.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.

Any forms used to gather personal data will be provided with a privacy notice (Appendix 1 and 2) and will indicate whether or not the individual needs to give consent for the processing.

A record will be kept documenting how and when consent was given.

If an individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then we will ensure that the processing of that data does not take place.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Parental consent will be sought prior to the processing of a child's data which would require consent until the age of 13, except where the processing is related to preventative or counselling services offered directly to a child.
Consent will be sought from the child after the age of 13 if we consider they have the competence to consent for themselves (often referred to as the Gillick competence test). If there is any doubt parental consent will continue to be required.

10. Subject access requests and other rights of individuals

Subject access requests

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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

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.

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

Responding to subject access requests

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student 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

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.
A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, 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)

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.

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 student) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around our sites 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 Executive Headteacher or Executive Business Manager.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.
We will obtain written consent from parents/carers, or students aged 13 and over, for photographs and videos to be taken of students 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 student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.
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.
See our child protection and safeguarding policy for more information on our use of photographs and videos.

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 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 (see section 6)
- 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
- 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, 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

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
- 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 students 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, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT policy and GDPR Data Security Guidelines for Staff (Appendix 4))
- 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)

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 data protection law.

17. Personal data breaches

The schools within our Federation 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 students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

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

The DPL and DPO are responsible for monitoring and reviewing this policy.
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 Federation's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- ICT Policy
- Child protection and safeguarding policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor, DPL or data processor must immediately notify the data protection officer (DPO) by emailing or phoning.
- 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
- 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 DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (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 the school's computer system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach

- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 stored on the school's computer system.
- 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
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

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/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

In other circumstances, for example a school laptop containing non-encrypted sensitive personal data being stolen or hacked, appropriate guidance will be sought and actions taken to remedy the situation in line with the outline approach above.

Appendix 2 - Data Security – Obligations of Staff

Data Security User Checklist

This checklist applies to CFF staff and governors.

This checklist refers to personal data belonging to Cumbria Futures Federation (Beacon Hill Community School and Solway Community Schools as the data controllers:

- No sensitive/special categories of data should be shared via any method without a prior discussion with the Business Manager and/or IT Manager to agree a secure method of transmission. Permission must be granted by the Executive Headteacher once a secure method has been agreed and **before** sending any data of this type.

- Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.

- Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).

- Paper records containing personal data **must** be kept secure if they are taken off the school premises and limited to low risk data.

- Users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically.

- Passwords **must** be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the school network and Office 365 Services.

- User names and passwords **must not** be shared.

- Electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.

- Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.

- Emails **must** be sent in a secure manner if they contain personal data.

- Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.

- Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.

- Visitors to areas of the school containing special categories of personal data **must** be supervised at all times.

- Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.

- Personal data **must not** be disclosed to any unauthorised third parties.

- Personal data **must not** be accessed through public WIFI.

- Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
    - It **must** be issued by Beacon Hill Community School
    - It **must** be encrypted when not being accessed;
    - It **must** be stored in a secure and safe place when not in use;
    - It **must not** be accessed by other users (e.g. family members) when out of school.

- Personal data **must** be securely deleted when no longer required.

- Personal electronic devices **must not** be used to hold personal data belonging to Beacon Hill Community School.

- Personal electronic devices **must** be password protected, have all required security updates installed, have up-to-date active anti-virus and anti-malware checking software before being used to access personal data belonging to Beacon Hill Community School via:
    - A password protected removable storage device;
    - The remote desktop protocol (i.e. remote access to the school network);
    - Office 365 (including Emails, OneDrive etc).

- No personal data should be copied, downloaded or stored on personal electronic devices.

- Personal electronic devices that have been set to automatically log into the school network, school email accounts or Office 365 services that are lost or stolen **must** be reported to the IT Manager immediately, so that access to these systems can be reset.

- One Drive can be used but copies of documents containing personal data **must not** be stored as local copies on the personal electronic device.

- If personal data is taken off Beacon Hill Community School premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.

- Before sharing personal data, Beacon Hill Community School staff and governors **must** ensure:
    - They are allowed to share it;
    - That adequate security is in place to protect it;
    - Who will receive the personal data has been outlined in a privacy notice.

- Any personal data archived on disks **must** be kept securely in a lockable cabinet.

- Beacon Hill Community School staff and governors are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

For the purpose of this document:
A “personal electronic device” is a device not owned by Beacon Hill Community School, but access by a member of staff or governing body.
I confirm that I have received, read and understood the guidance above relating to data security.
Name:
Date:

Appendix 3 – Privacy Notice – Students and Parents (Solway's Privacy Notice attached as example)

GDPR Privacy Notice (How we use student information)

Introduction

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

Personal data is information that identifies someone as an individual and relates specifically to that person. Solway Community School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to students and their families is to be processed.

This privacy notice explains how we collect, store and use personal data about students. It also explains the decisions that you can make about your own information.

Our **Data Protection Officer** is Dale Stephenson. Our **Data Protection Lead** (dealing with internal policies, processes and queries) is Jennifer Rowlands (see 'Contact us' on page 4).

The categories of student information

Personal data that we may collect, use, store and share (when appropriate) about students includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Assessment information (such as reports, feedback, test data and exam results)
- Student and curricular records
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Special Educational Needs information (such as Education and Health Care Plans (EHCPs), Individual Education Plans (IEPs) and notes from review meetings and professional assessments)
- Exclusion & behavioural information
- Record of achievement & rewards
- Details of any medical conditions including physical and mental health (such as medication details, allergies, and notes from meetings/GPs/other health care professionals)
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers (such as Early Help Assessments)
- Post 16 learning information and destination data
- Photographs & videos
- CCTV images captured in school

Why we collect and use this information

We use the student data to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care
- Protect student welfare
- Assess the quality of our services
- Administer admission waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use students' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

- Less commonly, we may also process students' personal data in situations where:
- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using students' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

We may also receive information about students from other organisations such as their previous school, local authority and/or the Department for Education (DfE).

Data security and storage of student information

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.

We keep personal information about students while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Our data protection policy sets out how long we keep information about students.

Sharing student information

The school routinely shares students' information with, but is not restricted to:

- Schools that the students attend after leaving us
- Our local authority (LA) Cumbria County Council
- The Department for Education (DfE)
- The student's family and representatives
- Educators and examining bodies
- Our regulator Ofsted
- Our partner school – Beacon Hill Community School
- Destination schools & colleges including alternative provision
- The NHS and other public health bodies
- Other public services that have a lawful right to collect student information
- Third parties where we have clear legal basis

Why we share student information

The school does not share information about our students with anyone without consent unless the law and our policies allow us to do so.

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

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

National Student Database

We are required to provide information about students to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Student Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education (DfE) with any further questions about the NPD.

Youth support services - students aged 13+

Once our students reach the age of 13, we are legally required to pass on certain information about them to Inspira as it has legal responsibilities regarding the education or training of 13-19 year-olds.
This information enables it to provide youth support services, post-16 education and training services, and careers advisers.
Parents/carers or students once aged 16 or over, can contact the school to request that we only pass the individual's name, address and date of birth to Inspira

Transferring data internationally

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.

Parents and students' rights regarding personal data

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.
Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.
Parents also have the right to make a subject access request with respect to any personal data the school holds about them.
If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form.

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
Parents/carers also have a legal right to access to their **child's educational record.**

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

If you would like to make a request or exercise any of these rights please contact our **Data Protection Officer or Data Protection Lead.**

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance using the Contact Us details below.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https: https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Further information

To download our Data Protection Policy please visit our website (www.beaconhill.cumbria.sch.uk).

If you require more information about how the local authority store and use your personal data:
www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp
To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools
If you cannot access these websites please contact the LA and/or DfE as follows:

Performance Unit,
Children's Services
Cumbria House
Botchergate
Carlisle
Cumbria
CA1 1RD
tel: 01228 221271
www.cumbria.gov.uk/childrenservices
ros.dean@cumbria.gov.uk
Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Tel: 0370 000 2288
www.education.gov.uk
htttp://www.education.gov.uk/help/contactus

Contact Us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Lead:**

- Mrs Jennifer Rowlands, Solway Community School, Liddell Street, Silloth, CA7 4DD
  Tel 016973 31234 or email jennifer.rowlands@solway.cumbria.sch.uk

For serious concerns, data breaches or complaints please contact our Data Protection Officer:

- Mr Dale Stephenson, Netherhall School, Netherhall Road, Maryport, CA15 6NT
  Tel 01900 813434

This notice is based on the Department for Education's model privacy notice for students, amended for parents and to reflect the way we use data in this school.

Appendix 4 – Privacy Notice – Staff (Beacon Hill version added for information)

Privacy Notice
(How we use school workforce information)

Introduction

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

Personal data is information that identifies someone as an individual and relates specifically to that person.

Beacon Hill Community School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to the school workforce is to be processed.

The school workforce includes all those employed to teach, or otherwise engaged to work, either on a paid, contracted or voluntary basis at Beacon Hill Community School.

This notice is to explain how and why we collect personal information about you and what we do with that information. It also explains the decisions that you can make about your own information.

Personal data is held by the school to assist in the smooth running of the school and/or enable individuals to be paid.

Our **Data Protection Officer** is Dale Stephenson. Our **Data Protection Lead** (dealing with internal policies, processes and queries) is Jennifer Rowlands (see 'Contact us' on page 4).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs & videos
- CCTV footage captured in school
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we collect and use this information

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils

- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Data security and storing workforce information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will review this file and delete the information in it in accordance with the school's Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

In some circumstances we may retain information for longer periods but we would only do so if we had good reason and only if we are allowed to do so under data protection law. e.g. for child protection issues.

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.

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred paper-based records, and override/delete electronic files.

Who we share this information with

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

We routinely share this information with, but is not restricted to:

- Our local authority Cumbria County Council
- The Department for Education (DfE)

- Other schools or organisations following reference requests
- Payroll provider
- Your family or representatives
- Our regulator Ofsted
- Educators and examining bodies
- Our partner school – Solway Community School
- Disclosure and Barring
- Other public services that have a lawful right to collect workforce information
- Third parties where we have a clear legal basis

Under the General Data Protection Regulation (2016/679 EU) (GDPR), personal data relating to criminal convictions and offences can be processed only:

- under the control of official authority; or
- when it is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

Why we share school workforce information

We are required to share information about our workforce members with our **local authority (LA)** under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

We share personal data with the **Department for Education (DfE)** on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools. All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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

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

To contact the department: https://www.gov.uk/contact-dfe

Transferring data internationally

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.

Your rights

How to access personal information we hold about you

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with

- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

If you would like to make a request or exercise any of these rights please contact our **Data Protection Officer** *(see Contact Us)*

Further information

To download our Data Protection Policy please visit our website (www.beaconhill.cumbria.sch.uk).

If you require more information about how the local authority store and use your personal data:
www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp

If you cannot access these websites please contact the LA and/or DfE as follows:

Performance Unit,
Children's Services
Cumbria House
Botchergate
Carlisle
Cumbria
CA1 1RD
tel: 01228 221271
www.cumbria.gov.uk/childrenservices
ros.dean@cumbria.gov.uk
Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Tel: 0370 000 2288
www.education.gov.uk
htttp://www.education.gov.uk/help/contactus

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance using the *Contact Us* details below.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https: https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact Us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Lead:**

- Mrs Jennifer Rowlands, Solway Community School, Liddell Street, Silloth, CA7 4DD
  Tel 016973 31234 or email jennifer.rowlands@solway.cumbria.sch.uk

For serious concerns, data breaches or complaints please contact our Data Protection Officer:

- Mr Dale Stephenson, Netherhall School, Netherhall Road, Maryport, CA15 6NT
  Tel 01900 813434

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.