

## | Student Data Collection

**Please Note:** this section also relates to some of the forms that need to be completed separately.

### DATA PROTECTION AND PRIVACY

The school is required to keep information about your child on its database and, under terms of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), we have a duty to ensure that this information is correct and up-to-date, and that we have a legal basis for processing the data; we take our responsibilities with regard to the protection of all personal data very seriously. For further information on the school's Information Policy (and all other school policies), please go to <https://www.cockermouthschool.org/about-us/school-policies>

All information provided by you is held on a secure, password-protected computer system and can only be accessed by school staff with the relevant permissions. The school is required to share some data with the Department for Education (DfE), which, in turn, may be shared with the Local Authority. For details of other third parties with whom we share data, please see the Privacy Notice section on page 23.

### STUDENT PERSONAL DETAILS

It is important that we have the correct student information and emergency contact details on our database so that you (or your delegated contact) can be contacted as quickly as possible should the need arise whilst your child is in school. All **new** students need to provide us with certain information which can be done in the following ways:

- By completing the electronic form available on our website (a link to this will be emailed to you)
- By completing a paper form (available on request).

Whichever method you choose, you will need to:

- Provide student personal details
- Provide emergency contact details
- Provide relevant student medical information
- Complete the consent section for Internet use, biometric data, educational visits, Youth Support Services, and use of student images and names for marketing.

**Existing Cockermouth School students need only provide this information if there have been any recent changes to personal data or consent.**

The **Student Details** section includes information that we are required to hold by law, such as student personal data and emergency contact details. For safeguarding purposes, we are required to hold a **minimum** of **three** emergency contacts for each student. **All** those with parental responsibility for the child should be listed as contacts (including parents, carers and social workers) regardless of home circumstances; we can only remove parental contacts if a court order has been issued that removes the parental rights of that contact. You can also add the details of any other persons who can be contacted during school hours in the event of an emergency, such as grandparents, other relatives, neighbours etc (a maximum of four contacts in total if possible). All contacts should be listed in the order in which you would like them to be contacted should an emergency occur. Consent should be sought from all contacts before you add their personal details to the data sheet.

The **Student Medical Information** section should be completed by you and includes doctor's surgery and telephone number, any medical conditions or disabilities of which the school should be aware, and details of any prescribed medication carried by your child in school (such as epipens, inhalers or oral medicines). If your child intends to carry medication or have medication administered in school, a member of the pastoral support team will contact you for further information. Depending on the nature of any medical conditions, you may also be asked to complete an **Individual Health Care Plan** for your child; again, a member of the pastoral support team will contact you in due course if this is the case.

### Changes to Student Details

Once your child has started at Cockermouth School, it is important that any changes to details are passed on to us as quickly as possible, especially changes of address and contact telephone numbers, as incorrect information may prevent us from being able to contact you in an emergency. There are several ways you can do this:

- Complete a contact form on Firefly (see page 13);
- Request a 'Change of Student Details' form from Reception, the Pastoral Support Office, or download a copy from Firefly at <https://cockermouth.fireflycloud.net/data-protectionstudent-details>;
- Send an email to [dataoffice@cockermouthschool.org](mailto:dataoffice@cockermouthschool.org) – please note, we can only accept changes to student details using this method from an email address already registered with us and if the student's full name and date of birth are included;
- Send in a letter with the amended details including your child's name, date of birth and form group addressed to the Data Office, c/o Cockermouth School.

If any changes to details are as a result of a family split (especially address changes) it would be helpful for us to be aware of this.

### ELECTRONIC COMMUNICATION

As part of our commitment to the *Reduce, Reuse, Recycle* ethos, we send all whole-school information home to parents via email using Edulink or Firefly where possible. This not only reduces paper usage (helping to protect the environment) but also significantly reduces printing costs. With this in mind, could you please enter an appropriate (i.e. parent or carer) email address in the space provided on the Student Details section that we can use as a primary email address (if parents share the same email address, enter this for one contact only). If you are unable to receive emails, please indicate on the sheet and we will continue to send paper copies of all relevant communications. We also ask that you supply a mobile telephone number in the relevant section so that text messaging can be used where appropriate (school closure, cancellation of fixtures/trips, attendance issues etc).

### SCHOOL PHOTOGRAPHS

The school invites an official photographer (Tempest) to come into school once a year to take photographs of our students. This serves two purposes: we attach an electronic copy of the photo to the student's personal details on our school database; and photo packs are also available for parents to purchase. This year, the photographer will be in school to photograph our Year 12 students on the first day of term on Wednesday 5 September 2024. You will receive a letter giving instructions on how to order packs, together with the photo proofs, during the first week of the Autumn Term.

### THE USE OF YOUR CHILD'S NAME, IMAGE AND VOICE

We may also take photos or videos of students during the course of a lesson as a teaching and learning tool, or during an event, educational visit or sporting activity to use in school displays or for marketing/school publicity purposes. We don't need parental consent to use personal data, including image or voice recordings when we use it for education purposes. Using the names, images and voices of students in their work and in displays inside school is a fundamental part of their education, personal development and how we celebrate them. This does not affect your or your child's statutory rights (as described in the Privacy Notice on page 23). Anyone can raise any concern with any member of staff about our use of their or their child's data at any time and we must ensure the rights of the individual are upheld if we have no good reason to refuse.

However, we **do** need parental consent to use personal data for other reasons such as marketing or self-promotion in publications and on websites or social media platforms (such as Facebook, Twitter and Instagram) directly managed by us or, with our permission, by others associated with us, and this may include pictures that have been drawn by students. Images that might cause embarrassment or distress will not be used, nor will image or voice recordings of your child be associated with materials or issues that are considered sensitive. You can ask to see any images that we hold of your child at any time.

Photography, audio recording or filming will only take place with the permission of the Headteacher or other senior manager, and under appropriate supervision.

Regardless of who is doing the publishing, our policy is that students will only be named if there is a reason to do so (e.g. they have won a prize), and no other personal details will be published or given out. If names will or might be published, e.g. in a newspaper article, we will check that you have given the appropriate consent at the time and before the publishing happens. It is important to understand that if you do consent, the images and your child's name will appear in local or national newspapers and worldwide online.

If you attend Cockermouth School functions and wish to take images of your child, please be sensitive to other people and try not to disrupt concerts, performances and events. Please also bear in mind that you may capture other people's children so make sure images are appropriate. **If you, or your child, intend to share images, you can only share them publicly (i.e. post them to social media) with the express permission of the parents of everyone in the images.**

Please also note that we ask all parents and students to support our approach to online safety and not upload or post to the Internet any pictures, audio, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute. If these rules are not respected, trustees reserve the right to stop everyone from recording school events.

Consent for the use of your child's name and image for the marketing and promotion of the school is sought via the Parental Consent form, which can be found in the accompanying booklet. This form also includes consent for Educational Visits, Emergency Pain Relief, Youth Support Services and Biometric Data. Consent, once given, can be withdrawn at any time by contacting the school Data Office on [dataoffice@cockermouthschool.org](mailto:dataoffice@cockermouthschool.org).

For all data collection issues and changes to student and contact details, please contact the Data Team on:

- [dataoffice@cockermouthschool.org](mailto:dataoffice@cockermouthschool.org)

## **BIOMETRIC CASHLESS CATERING AND LIBRARY MANAGEMENT SYSTEM**

(This section should be read by both the student and parents)

Cockermouth School uses a voluntary biometric recognition system for administration functions for cashless catering and library management. We find this provides us with a number of very significant benefits including:

- Students do not have to remember a PIN or to bring a card;
- Reduction in administration time and cost dealing with lost or forgotten cards/passwords/PINs;
- Reduction in the need for cash handling;
- Reduction in queuing time.

In order to comply with the provisions of the Protection of Freedoms Act 2012, we need written permission from a parent/carer in order for students to use the biometric system. Please complete the relevant slip in the accompanying booklet. Alternatively, consent can be emailed to [dataoffice@cockermouthschool.org](mailto:dataoffice@cockermouthschool.org).

We will continue to offer an opportunity to opt-out for those students who would prefer to use alternative forms of identification.

**Background to the use of Biometrics in School:** For the sake of clarity, biometric information is information about someone's physical or behavioural characteristics that can be used to identify them. There are many possible biometrics, including for example, a digital photograph, fingerprint, or hand shapes. As part of our identity management systems, we currently record a biometric measurement taken from a finger, *but not a fingerprint image*. The information is stored in a highly secure database and is only used by the school to confirm who is using a range of services. In future we may use other biometric services where appropriate. Our chosen solution allows us to use a secure database holding

biometric data for use with a range of services. This means we store the least amount of data possible. This reduces the risk of loss of data.

The school will not use the biometric information for any purpose other than that stated above. The school will store the biometric information collected securely in compliance with the UK GDPR and DPA. The school will not share this information with anyone else and will not unlawfully disclose it to any other person. The data that is held cannot be used by any other agency for any other purpose.

**Current Legislation – The Protection of Freedoms Act 2012:** This legislation requires schools to:

- Inform parents about the use of the biometric systems in the school and explain what applications use biometrics;
- Receive written permission from one parent if the school is to continue processing biometrics for their child;
- Allow children to choose an alternative way of being identified if they wish.

Children under 18 who do not have permission will not be able to use existing or new biometrics when using services in the school.

If you do not wish your child to use the biometric system, or your child chooses to use an alternative form of identification, we will provide reasonable alternative arrangements that allows them to access current and future services in the form of a PIN (Personal Identification Number).

Should you agree to your child using the biometric system, it is important that you return the signed consent form (in the accompanying booklet or via Edulink) as soon as possible. Please note that when your child leaves the school, or if for some other reason they cease to use the biometric system, their biometric data will be permanently deleted.

If you would like more information, please contact:

- Mr A Westley, Network Manager, 01900 898888, [westleya@cockermouthschool.org](mailto:westleya@cockermouthschool.org)

## **ACCEPTABLE USE POLICY (AUP): INTERNET, MOBILE DEVICES, ICT FOR STUDENTS**

*(This section should be read by both the student and parents)*

As part of the school's IT programme, Cockermouth School offers students supervised access to the Internet during lessons and at the teacher's discretion. Before being allowed to use the Internet, all students must obtain parental permission, and both students and their parents must sign and return a declaration and permission form as evidence of parents' approval and the student's acceptance of the school rules on this matter.

Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. The school employs its own internet monitoring and filtering system, Smoothwall, which helps us to provide a safer browsing experience for all students.

Whilst our aim for Internet use is to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and carers of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, staff will guide students towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

Cockermouth School strongly believes in the educational value of electronic services and recognises their potential to support its curriculum and student learning by facilitating resource sharing, innovation and communication. Cockermouth School provides its students with the means of using personal tablets

or laptops at school to be used in selected classrooms under the direct supervision of their teacher. Cockermouth School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of Cockermouth School's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The guidance below should be read by both student and parents/carers before completing the declaration and permission form, which can be found in the accompanying booklet, before any devices can be connected to the school network.

For the purpose of this policy, the term ICT Acceptable Use Policy (AUP) will be used to reference the Acceptable Use Policy: Internet, Mobile Devices, ICT for students.

**To whom does this policy apply?** This policy applies to all students of Cockermouth School who may have access to a school-owned computer or network resources via a personal mobile device, regardless of whether or not they use it in their day-to-day school work routine.

**Why is this document necessary?** All organisations (including schools) where computers are in use are required to have a code of practice such as this. It is necessary to outline the principles underpinning appropriate computer use, make expectations clear and ensure users are fully aware of the consequences of not following the code of practice and computer misuse. This acceptable usage policy has been put together to provide guidance to all students (and parents or carers) on what is appropriate use of ICT within Cockermouth School.

**How is this policy communicated and updated?** The ICT Acceptable Use Policy (AUP) is published on the Cockermouth School website and a copy is given to each student when they join the school as part of the induction process. Each student and their parents are required to sign the ICT AUP Agreement form, which can be found in the accompanying booklet, and return this to the Data Office, signifying their acceptance of the policy, before they can be given an account with access to the network. In signing, they accept that they agree to all amendments, which will be published on the school's website, unless the Data Office is notified in writing by the individual.

When the ICT AUP is updated, a new version is provided to all students electronically and published on the website. Paper copies are also available from the Network Manager or the Data Office.

**What are the consequences of improper conduct?** Failure to abide by this AUP will be treated in the same way as any other misconduct issue.

#### **General Computer Use:**

- In general, use of ICT equipment (such as computers, printers and tablets), email and the Internet within the school should be primarily to enhance learning.
- Use for business purposes not related to school activities or personal gain is not permitted.

#### **User Accounts:**

- User accounts are the responsibility of the student.
- Passwords and lock codes must be kept secure.
- Passwords must not be written down or disclosed to anyone.
- Students must not allow anyone else to use their account, nor should they use anyone else's account.
- Students must log off their computer and lock their device when away from their machine. Accounts are not to be left logged in and unattended.

#### **Hardware and Software:**

- All students are responsible for the care and safe-keeping of any ICT equipment.
- Keep all liquids and food away from any ICT equipment and be aware of the health and safety hazards relating to electrical equipment.
- Students should report all computer faults to their class teacher as soon as they are identified.

#### **Internet Usage:**

- All use of the Internet within the school should be primarily to enhance learning.

- Use of the Internet within the school for the conducting of private business or personal gain is not permitted.
- Students are not permitted to use the Internet for any illegal activity; although not specifically against the law, this includes accessing sites meant for adults of 18 years or older such as pornographic and gambling websites.
- Students must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material.
- The downloading of any *unlicensed* material such as music, video, TV programmes, games, pdf files is illegal and, therefore, not permitted.

#### **Email:**

- All students are provided with a **@cockermouthschool.org** email account. Its use must be limited to school-related work only, and not be used for personal correspondence or for signing up to non-school-related Internet services or accounts.
- This email is accessible from within Cockermouth School via the network using Outlook or Outlook Web Access and via the Internet using Outlook Web Access (OWA).
- Attachments on emails are limited to 30MB. If you wish to send anything over this size, please contact IT Support who can arrange to compress the file for you or find an alternative way of sending data.
- Students are responsible for the day-to-day management of their emails, being aware of the data storage limits and ensuring unwanted material is deleted on a regular basis.
- If email is being accessed using OWA from a personal or public use computer:
  - Do not store anything on the computer hard-drive.
  - Be careful who can see what you are doing if accessing in public place.
  - Make sure you log off completely.
- Email should be treated as inherently insecure.
- As with any form of correspondence, be aware of the language used.
- Do not open or forward any email or attachment from an unrecognised source or that you suspect may contain inappropriate material or viruses.
- Do not respond to emails that request personal details unless you are confident the source is genuine.
- Students must not send, forward, print or transmit in any form any offensive, obscene, violent, dangerous or inflammatory material via email.
- Students are not permitted to send or forward chain letter emails, jokes, spam etc.
- If you are concerned about any email that you may have received, contact IT Support, or tell any other member of staff.

#### **Email and Internet Filtering and Monitoring:**

- The school has in place a sophisticated filtering & monitoring system that:
  - Checks for viruses and traps suspicious emails.
  - Denies access to most undesirable and inappropriate sites on the Internet.
  - Maintains a list of banned sites, which is updated on a regular basis.
 Whilst this provides a measure of reassurance it must be understood that the filter does not trap or block everything.
- Please be aware that:
  - Student emails to and from the school can and will be monitored for inappropriate use.
  - Internet access within the school can and will be monitored for inappropriate use.
  - All Internet sites accessed by students are logged with date and time of access.
- Misuse of the Internet and/or email will always result in an investigation and may lead to disciplinary action.
- The accessing and use of inappropriate and indecent materials from the Internet or via e-mail will result in disciplinary action being taken.

#### **Social Networking Sites:**

- Access to social networking sites is not allowed.

#### **Bullying/Cyber-bullying/Online Bullying:**

- The school will not tolerate any form of bullying, including electronic or online bullying.

- The misuse of email systems or the Internet for harassing people, such as by sending unpleasant or aggressive messages ('cyber bullying'), is on the increase. The school reserves the right to monitor all Internet and email activity within the bounds of current legislation in order to keep the Internet safe for all at Cockermouth School, and to protect from online bullies. It is a condition of this policy that all users of our network accept that Internet activity is monitored as well as filtered.
- Any instances of bullying will be taken very seriously. As with any other form, cyber or online bullying (involving the use of personal computers, mobile phones etc) will be investigated fully and will result in disciplinary action.

#### **Pornography & other inappropriate material:**

- Students are not permitted to access or save any form of pornography or offensive, obscene, violent, dangerous or inflammatory material onto computers.
- Students must not store personal data on the school network. This includes, but is not limited to, photographs, videos, music and documents.
- IT Support reserve the right to perform spot checks on students' accounts and computers at any time.
- If any inappropriate material is found, the account will be disabled immediately and disciplinary action will begin.

#### **Mobile Phones:**

In order to enhance our safeguarding of young people, as well as to protect their wellbeing, avoid unnecessary distraction from their learning and improve students' positive interactions with others, mobile phones must not be used by students while they are on the school site.

- Mobile phones must not be used by students while they are on the school site.
- Mobile phones, which are brought into school, must be turned off and stored out of sight (in a bag or locker, not pockets) immediately as the student arrives at the school gate. They must remain turned off, and out of sight, until the student has left the site at the end of the day.
- If a mobile phone is seen by a member of staff, that member of staff will be required to confiscate it. The member of staff will log the confiscation on Class Charts and place the mobile device at reception for safe storage.
- A student using headphones or accessing their phone through a smartwatch will also have their phone confiscated, as this would indicate they have been using their phone.
- When a mobile phone is confiscated the mobile phone policy protocols will be followed. A member of the school's administration team will contact a parent or carer to inform them of their child's phone confiscation. The phone will be made available for collection by a parent or carer. Mobile phones will only be returned to a parent, carer or nominated adult.
- Where parents or carers need to contact students during the school day, they should do so on the school telephone system via reception.
- Where a mobile phone is confiscated on multiple occasions, a meeting will be arranged for parents or carers to meet with a senior member of staff in school.
- Phones should not be visible after 3.30pm on the school site. If a student is seen using a mobile phone after 3.30pm, the member of staff will ask them to put their phone away and the student will then be issued with a mobile phone detention on Class Charts. For students that persistently use their mobile phone after school, sanctions will escalate.
- One exception is that students in our Sixth Form can use their mobile phone within our dedicated Sixth Form facilities.

#### **Hacking:**

- The Computer Misuse Act 1990 makes it illegal to:
  - Gain unauthorised access to a computer's software or data (hacking), including the illegal copying of programs.
  - Gain unauthorised access to a computer's data for blackmail purposes.
  - Gain unauthorised access to a computer's data with the intention of altering or deleting it, including planting viruses.
  - Copy programs illegally (software piracy).
- Any type of hacking (defined as attempt to gain access to folders, databases, or other material on the network to which one is not entitled) is considered to be an extremely serious offence.

- To comply with the Computer Misuse Act 1990 any user who indulges in hacking or is found with hacking software/paraphernalia on their computer or network account is liable to be subject to disciplinary action.
- Likewise, physical interference with another user's computer or school-owned computer will not be tolerated.

## **Appendix A: Legislation & Regulations**

**The Computer Misuse Act (1990)** states that the following actions are illegal:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.


## **PRIVACY NOTICE: HOW WE USE PARENT & STUDENT INFORMATION**

*This Privacy Notice has been written to inform parents and students of Cockermouth School about what we do with your personal information. This Notice may be subject to change. For the purpose of this Notice, where 'parent' is stated, this includes anyone with parental responsibility for a student such as birth or adoptive parent, foster carer (local authority or private), legal guardian.*

### **Who are we?**

Cockermouth School is a 'Data Controller' as defined by Article 4 (7) of UK GDPR. This means that we determine the purposes for which, and the manner in which, your personal data are processed. We have a responsibility to you and your personal data, and will only collect and use this in ways that are compliant with data protection legislation.

The school has appointed Veritau Ltd to be its Data Protection Officer (DPO). The role of the DPO is to ensure that the school is compliant with UK GDPR and the Data Protection Act 2018 and to advise on data protection procedures. If you would like to discuss anything in this privacy notice, please contact our school Data Manager on [dataoffice@cockermouthschool.org](mailto:dataoffice@cockermouthschool.org), or Veritau Ltd. Veritau's contact details are:

<p>Schools Data Protection Officer Veritau Ltd West Offices Station Rise York North Yorkshire YO1 6GA</p> <p><a href="mailto:schoolsDPO@veritau.co.uk">schoolsDPO@veritau.co.uk</a> 01904 554025</p> <p><i>Please ensure you include the name of your school in all correspondence</i></p>	
--	---

### **What information do we collect?**

The personal data we collect about you includes (but is not limited to):

- Personal identifiers and contact details, including name, postal address, email address, phone number, date of birth and student number.
- Educational and assessment attainment, such as national curriculum assessments (Key Stage 2), Reading and Literacy assessments, academic progress data, GCSE and GCE results, and post-16 courses.
- Characteristics such as ethnicity, language, free school meal and pupil premium eligibility.



- Attendance information, including sessions attended, reason and number of absences, and previous schools attended.
- Behavioural information, including management plans, exclusions and any relevant alternative provision put in place.
- Safeguarding information including, but not limited to, court orders and professional involvement and support.
- Child in Need or Looked After status, including episodes of being looked after or a child in need, adoptions, care leavers and outcome information.
- Special Educational Needs and Disability information.
- Healthcare and medical information such as doctor details, allergies, medication and dietary requirements.
- Photographs or video image and voice recordings for assessment and celebration, and CCTV footage for safety and security reasons (please see section on Student Images at the end of this Notice).
- Information relating to school trips and extra-curricular activities.
- Records of communications and interactions we have with you.
- Biometric data e.g. thumbprints or facial recognition.
- Medical information relevant to pandemic management, such as your vaccination status and positive test results (where relevant).
- E-monitoring information about your use of the school's network and IT systems.
- Financial information like bank details and entitlement to meals, transport and premium funding to manage catering, school trips etc.

### **Why do we collect and use your personal data?**

In order to fulfil official functions and to meet legal requirements, we process your information to:

- support student learning;
- meet our safeguarding obligation to students (e.g. food allergies, emergency contact details, CCTV);
- monitor and report on student attainment progress;
- provide appropriate pastoral care;
- assess the quality of our educational provision;
- meet the statutory duties placed upon us regarding DfE data collections;
- prevent the spread of infection and maintain adequate and safe student and staffing levels (during a pandemic);
- celebrate or promote the school, including in newsletters, on the school website and social media platforms, including for scientific interest or to record our own school history;
- control access to services e.g. biometric controlled catering services.

### **What is our lawful basis for processing your information?**

Under the UK GDPR, it is essential to have a lawful basis when processing personal information. We normally rely on the following lawful bases:

- Article 6(1)(a) – consent
- Article 6(1)(c) – legal obligation
- Article 6(1)(e) – public task

Where we are processing your personal data with your consent you have the right to withdraw that consent. If you change your mind or are unhappy with our use of your personal data, please let us know by contacting the school's Data Manager.

There may be occasions where our processing is not covered by one of the legal bases above. In that case, we may rely on Article 6(1)(f) - legitimate interests. We only rely on legitimate interests when we are using your data in ways you would reasonably expect.

Some of the information we collect about you is classed as special category data under the UK GDPR. The additional conditions that allow for processing these data are:

- Article 9(2)(a) – explicit consent
- Article 9(2)(g) – reasons of substantial public interest

The applicable substantial public interest conditions in Schedule 1 of the Data Protection Act 2018 are:

- Condition 6 – statutory and government purposes
- Condition 10 – preventing or detecting unlawful acts
- Condition 18 – safeguarding of children and vulnerable people

### **Who do we obtain your information from?**

We normally receive this information directly from you, for example via admissions forms, or secure file transfer from a previous school. However, we may also receive some information from the following third parties:

- Department for Education (DfE).
- Local Authority.
- Other agencies working with the child/family, such as Children's Services, the Police, Health Services etc.

### **Who do we share your personal data with?**

We may share your information with the following organisations:

- Schools/education providers that the students attend after leaving us, to support their continuing education;
- Our Local Authority, to ensure they can conduct their statutory duties such as under the [Schools Admission Code](#), including conducting Fair Access Panels, and careers guidance legislation;
- Department for Education (DfE), to help decide our school funding, monitor attainment & benchmark it nationally, compile league tables, develop national education policy and monitor it;
- National Health Service (NHS), for vaccinations, Education Health Care Plan (EHCP) provision;
- Government departments like UK Health Security Agency, local authority public health, and District Council Environmental Health Departments to comply with the law and support public health action;
- Youth support services, where relevant e.g. careers advice.
- Other agencies working with the child/family, where appropriate e.g. Children's Services.
- Exam Boards and other Awarding Bodies.
- School suppliers and IT applications, where necessary.

For more information on information sharing with the DfE please visit the [DfE website](#).

We may also share information with other third parties where there is a lawful basis to do so. For example, we sometimes share information with the police for the purposes of crime detection or prevention. We also regularly share information with appropriate organisations for the purposes of arranging school trips. Appendix 1, at the end of this Notice, lists some of the other third parties with whom we share personal data for educational purposes.

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so. The laws listed in this Notice that require us to collect information also require us to share it. Unless otherwise stated, data are transferred securely by hand delivery or registered post, via a government data transfer system like School to School, or via a contractor's secure data sharing system such as Wonde.

### **Sharing with Youth Support Services**

**Students aged 13+:** Once our students reach the age of 13, we pass information to our provider of youth support services (Inspira) as stipulated under section [507B of the Education Act 1996](#). The information provided is limited to the child's name, address, date of birth, and the name and address of a parent. Parental consent is not required to share these data but consent is required for any other

information relevant to the provision of youth support services. The right of consent is transferred to the student once they reach the age of 16 (see consent form in Appendix 2).

**Students aged 16+:** We will also share certain information about students aged 16+ with our local authority and/or provider of youth support services because they also have responsibilities in relation to the education or training of 13–19-year-olds under the same section 507B of the Education Act 1996. The information shared is limited to the student's name, address and date of birth, and the name and address of a parent. Parental consent to share these data is not required but we do need a student's consent to share any other information about them that is relevant to the provision of youth support services.

Providing this information enables Inspira to provide:

- youth support services;
- careers advisers;
- post-16 education and training providers.

All data are transferred to the youth support service (Inspira) via secure email or by Royal Mail delivery. For information on how data are stored by Inspira, please read the privacy notice on their website at: <https://www.inspira.org.uk/privacy-policy>.

*For more information about services for young people, please visit:*

- <https://www.inspira.org.uk> or
- <https://nationalcareersservice.direct.gov.uk/about-us/home>

**Department for Education:** The DfE collects personal data from educational settings and local authorities via various data collections. We are required to share information about our students with the DfE either directly or via our local authority for the purpose of those data collections under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data are transferred securely and held by the DfE under a combination of software and hardware controls, which meet the current [government security policy framework](#). For more information, please see 'How Government uses your data' section below.

**Local Authorities:** We may be required to share information about our students with the local authority to ensure that they can conduct their statutory duties under

- the [Schools Admission Code](#), including conducting Fair Access Panels.

#### **How long do we keep your personal data for?**

We will retain your information in accordance with our Records Management Policy and Data Retention Schedule (<https://www.cockermouthschool.org/about-us/school-policies>). The retention period for most of the information we process about you is determined by statutory obligations. Any personal information, which we are not required by law to retain, will only be kept for as long as is reasonably necessary to fulfil its purpose.

We may also retain some information for historical and archiving purposes in accordance with our Records Management policy.

#### **International transfers of data**

Although we are based in the UK, some of the digital information we hold may be stored on computer servers located outside the UK. Some of the IT applications we use may also transfer data outside the UK.

Normally your information will not be transferred outside the European Economic Area, which is deemed to have adequate data protection standards by the UK government. In the event that your information is transferred outside the EEA, we will take reasonable steps to ensure your data is protected and appropriate safeguards are in place.

### **What rights do you have over your data?**

Under the UK GDPR, parents and students have the following rights in relation to the processing of their personal data:

- To be informed about how we process your personal data. This notice fulfils this obligation.
- To request a copy of the personal data we hold about you.
- To request that your personal data is amended if inaccurate or incomplete.
- To request that your personal data is erased where there is no compelling reason for its continued processing.
- To request that the processing of your personal data is restricted.
- To object to your personal data being processed.

Please be aware that usually students are considered to have the mental capacity to understand their own data protection rights from the age of 12 years old. The school may therefore consult with a student over this age if it receives a request to exercise a data protection right from a parent. All information requests should be made to the Data Manager, preferably in writing.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact our DPO using the details provided above.

If we cannot resolve your concerns then you may also complain to the Information Commissioner's Office, which is the UK's data protection regulator. Their contact details are below:

Phone: 0303 123 1113. Opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form or live chat on [Contact us | ICO](#).

### **Changes to this notice**

We reserve the right to change this privacy notice at any time. We will normally notify you of changes that affect you. However, please check regularly to ensure you have the latest version. This privacy notice was last reviewed in March 2023.

## **ADDITIONAL INFORMATION**

### **How Government uses your data**

The student data that we lawfully share with the DfE through data collections:

- Underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- Informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or student progress measures).
- Supports 'longer term' research and monitoring of educational policy (for example, how certain subject choices go on to affect education or earnings beyond school).

### **Data collection requirements**

To find out more about the data collection requirements placed on us by the DfE (for example, via the school census) go to: [www.gov.uk/education/data-collection-and-censuses-for-schools](http://www.gov.uk/education/data-collection-and-censuses-for-schools).

### **The National Pupil Database (NPD)**

Much of the data about students in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the DfE and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to: [www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information](http://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information).

### **Sharing by the Department**

The law allows the DfE to share students' personal data with certain third parties, including:

- Schools and Local Authorities.
- Researchers.
- Organisations connected with promoting the education or wellbeing of children in England.
- Other Government departments and agencies.
- Organisations fighting or identifying crime.

For more information about the DfE's NPD data sharing process, please visit: [www.gov.uk/data-protection-how-we-collect-and-share-research-data](http://www.gov.uk/data-protection-how-we-collect-and-share-research-data).

Organisations fighting or identifying crime may use their legal powers to contact the DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, the DfE typically supplies data on around 600 students per year to the Home Office and roughly one per year to the Police.

For information about which organisations the DfE has provided with student information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police, please visit: <https://www.gov.uk/government/publications/dfe-external-data-shares>.

### **How to find out what personal information the DfE holds about you**

Under the terms of the Data Protection Act 2018, you are entitled to ask the DfE:

- If they are processing your personal data.
- For a description of the data they hold about you.
- The reasons they are holding it and any recipient it may be disclosed to.
- For a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the DfE, you should make a 'subject access request' to them. Find out how in the DfE's personal information charter published at: [www.gov.uk/government/organisations/department-for-education/about/personal-information-charter](http://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter)

To contact the DfE go to: [www.gov.uk/contact-dfe](http://www.gov.uk/contact-dfe).

### **Sharing data with other third parties**

It may be necessary for Cockermouth School to share data with some third parties outside of the DfE who, for example, provide software that helps with the day-to-day running of the school. A list of examples of companies with whom we regularly share data can be found with the privacy notice in the Policy section of the school's website: <https://www.cockermouthschool.org/about-us/school-policies>

