

Cherrywood Community Primary School

Hampshire



Data Protection Policy

Adopted on:	13 July 2026
Signed on behalf of the Governing Body	Mrs. B Read Chair
Review Date	July 2028

1.Introduction

Aim

This policy sets out how, why, and what personal data (also known as personal information) Cherrywood Community Primary School (“the school”)collects, how it uses it, and what the rights of the individual (**data subject**) are in relation to the personal data which the School collects.

This policy applies to all personal data however it is collected, used, recorded, and stored by the school, and regardless of whether it is in paper or electronic form.

This policy meets the requirements of the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 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](#).

The School uses CCTV cameras to protect its buildings and grounds and manage access to its site. Therefore, the policy also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information.

Data Controller

The school is the data controller of the personal data it collects.

Data Protection Officer

The School has appointed a data protection officer (DPO), Mrs. T Gray who may be contacted at admin@cherrywood.hants.sch.uk or via the school office on 01252 547896.

2.What is Personal Data or Personal Information

Personal information or data means any information relating to a specific individual (or one who can be identified from the data) and includes but is not limited to:

- name
- address
- date of birth
- photograph
- bank details.
- passport/driving license information
- online IDs

and any other information that identifies them.

Special Category Data

Special category data (formerly sensitive personal data) is personal information which is considered to be more sensitive and/or to require more protection. This includes information such as:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics, biometrics (where used for ID purposes)
- health
- sex life or sexual orientation.

The GDPR prohibits the collection, use and sharing of such information, except on specified and limited grounds (see below Section 4).

3.Data protection principles

The GDPR is based on data protection principles that School must comply with.

The principles say that personal data must be:

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

4.Collecting personal data

Legal reasons for collecting and processing personal data

We will only process/collect personal data where we have one of 6 legal reasons to do so under data protection law:

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

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

What data do we collect and why?

The school collects personal data about staff, pupils, parents, families and carers, governors, volunteers, third party suppliers and contractors, and visitors and other individuals who come into contact with the school. This information is gathered in compliance with the 6 legal reasons to:

- enable the school to fulfill its legal obligations to provide education to the pupils in the school, make them secondary school ready, support their social, moral, cultural, spiritual, and economic development, and to enable them to participate in the wider community.
- ensure the health, well-being, and safety of all pupils (and where appropriate their siblings and/or families and carers) and other school stakeholders including staff, and where appropriate, volunteers and visitors.
- enable the school to administer and comply with its legal obligations under contracts of employment and third-party contracts for services or supply.
- permit staff and governor training and development.
- ensure the security of the school site, the premises, and assets of the school.
- enable the school to provide facilities and services ancillary to its main functions (such as suitable IT and catering services).

Additionally, the School collects personal data to enable it to comply with its legal reporting obligations on matters such as pupil numbers, pupil attendance, and pupil performance data.

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, which include:

- compliance with employment and/or social security law
- it is in the vital interests of the data subject
- processing is of information that has been disclosed publicly by the data subject
- it is necessary for preventive medical or occupational health needs, or the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance, or
- where consent is given.

The school offers access to certain online services to pupils, such as classroom apps and online learning tools (such as Google Classroom, Timetable Rock Stars, Tapestry, Dojo, and Prodigy Maths). We intend to rely on parental consent as a basis for processing the information collected to make these facilities available.

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals (or in the case of pupils to their parents and carers) when we first collect their data, for example in the case of pupils, when they first join the school. 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.

5. Sharing personal data

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

- There is an issue with a pupil or parent, family and/or carer that puts the safety of the pupil, other pupils, and/or our staff at risk.
- We need to liaise with other agencies (we will obtain consent if necessary and/or permissible)
- 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.
 - 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.
- where disclosure is required to satisfy our obligations under the Education Acts
- research and statistical purposes, provided that 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 pupils or staff.

The school will not transfer personal data to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

6. 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 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 will the data be stored for, or if this is not 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 or email 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 **below** the age of 12 are generally not 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 pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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

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

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.

7. 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.

8. CCTV

The school uses CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the Business Manager via the School Office.

9. Photographs and videos

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

We will obtain written consent from parents/carers at the point of school admission for photographs and videos to be taken of pupils for communication, marketing, and promotional materials. This also includes images and video being placed on our website.

Where we need additional parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and (where appropriate in terms of capacity to understand) the pupil.

Uses may include:

- Within school on noticeboards, electronic displays, 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

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.

10. Compliance with Data protection obligations

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

- Appointing a suitably qualified/trained 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 sections 4 and 5)
- Issuing Privacy Notices (see Appendices 1 - 5)
- 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 (including Governors) 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.

11. 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 are not 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, (for example for Child protection conferences) staff will ensure it is kept secure at all times. Medical, or similar information, which is needed on a school trip, will be signed in and out of the School Office by the teacher leading the trip.
- School laptops and computers are password protected and staff are required to log-out/lock these devices to prevent unauthorized access. Staff 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 will not take paper copies of records such as assessment records, pupil progress information or documents which contain personal data off site (except as noted above); these must be accessed using the school secure access or stored on encrypted USB. No school laptops, UBS or other portable devices will be left unattended at any time when off the school site and will not be left in cars.
- Staff will only use their own personal devices in exceptional circumstances (such as when working off-site and are unable to access the school system via their UBKey/do not have access to a school provided encrypted USB). Any personal information accessed/processed will only be stored on their personal devices temporarily and staff are expected to follow the same security procedures as for school-owned equipment, and to comply with the School's IT Acceptable Use Policy.
- 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.

12. Retention and Disposal of records

Personal data will be retained for the periods set out in the School's Retention Schedule (a copy of which can be accessed via the School Office).

Personal data that is no longer needed or which can no longer be retained will be disposed of securely, usually cross-shredded or placed in a burn bag. 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.

13. Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 6.

Where appropriate, we will report the data breach to the ICO within 72 hours.

14. 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.

15. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. The Governing Body also retains an overall supervisory role and will audit the proper operation of the policy annually.

This policy will be reviewed every 2 years.

16. Complaints

Complaints will be dealt with in accordance with the School's Complaints Policy. Complaints relating to the handling of personal data may be referred to The Office of the Information Commissioner, Wycliff House, Water Lane, Wilmslow, Cheshire SK9 5AF, or online at www.ico.gov.uk.

17. Contacts

If you have any queries in relation to this policy, please contact the DPO via the School Office.

Re- approved on: 13th July 2026

Signed on behalf of the Governing Body by:

Chair of Governors

Appendices:

1 Privacy Notice - Pupils

2 Privacy Notice - Parents

- 3 Privacy Notice - School Workforce including volunteers.
- 4 Privacy Notice - Governors
- 5 Privacy Notice - Visitors, contractors and suppliers
- 6 Personal Data Breach Procedure

Related Policies/Documents

ICT Acceptable Use
Online Safety
A1
Staff Code of Conduct
Mobile Phone Usage
Communication and Contact Form
Photographic Consent Form

Appendix 1: Privacy Notice - Pupils

(How we use Pupil Information)

The purpose of this Privacy Notice is to explain why we collect information, what information we collect, and how/why we might share it.

Please read this in conjunction with our Data Protection Policy.

The categories of personal information that we collect, hold and share include:

- Personal information of pupils (such as name, unique pupil number and address)
- Emergency contact details
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility for pupils)
- Attendance information (such as sessions attended, number of absences and absence reasons) and exclusions.
- Assessment and progress information

- Relevant medical information
- Special educational needs information
- Behaviour information
- Welfare needs information.
- Safeguarding and child protection information
- Participation in school provided clubs including breakfast club and other co-curricular activities both on and off-site.
- Photographic and similar records of the pupils' engagement in school activities (both on and off-site)
- CCTV images captured on the school premises/by school CCTV.

We may also hold information about pupils that we have received from other organisations, including other schools, local authorities, and the Department for Education (DfE)

Why do we collect and use personal information?

We collect and use personal information to:

- Support pupil learning.
- Monitor and report on pupil progress.
- Provide appropriate pastoral care.
- Safeguard and care for the pupils and other vulnerable individuals.
- Allow the school to access support (both practical and financial) for pupils.
- Allow the school to plan for and appropriately support the welfare, health, emotional and social, as well as educational needs of pupils and families.
- Access support for pupils and families from third party/external agencies
- Monitor pupil attendance and behaviour.
- Administer admissions and potential waiting lists.
- Allow the school to access/provide sporting, cultural and other co-curricular activities/experiences to pupils.
- Allow the school to provide lunch services.
- Allow the school to plan for and monitor access to and usage of Breakfast Club
- Allow the school to plan and monitor access to and usage of clubs/co-curricular activities.
- Assess and monitor the quality of teaching and learning.
- Meet equalities legislation obligations.
- Ensure accessibility for pupils.
- Enable pupils to have access to and maintain access to appropriate online facilities.
- Provide evidence of/record and celebrate the achievements of pupils and the school.
- Protect the individuals working in and/or visiting the school and the integrity of the premises and school assets.
- Ensure the Governing Body has sufficient information to carry out its statutory duties.
- Support school improvement.
- Assess the quality of our services and how well our school is doing.
- Assess and monitor the effectiveness of our school strategic plans.
- Statistical forecasting and planning including income.
- Allow the school to comply with its obligations to provide information to the local education and other education authorities/bodies.
- Comply with the law regarding data sharing.

The lawful basis for collecting and using personal and other information.

We only collect and use pupil personal information when the law or our policies allow us to do so.

The General Data Protection Regulation allows us to collect and use personal and other information where:

- we are complying with a legal requirement,
- processing is necessary to protect the vital interests of a data subject or another person,
- where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and
- It is in the substantial public interest to do so.

Less commonly, we may also collect, hold, and use pupil data where we have obtained consent to use it in a certain way.

Where we have obtained consent to use pupils' personal information, 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.

Our requirement for this data and our legal basis for processing this data also include the Education Act 1996, 2002 and 2011, The Children's Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998, and the Equalities Act 2010.

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

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Storing personal data

We keep pupil personal data while they are attending Cherrywood Community Primary School (or whilst they are seeking a place at the school). We may also keep it beyond their attendance at our school if this is necessary to comply with our legal obligations. Our Retention Schedule sets out how long we keep information about pupils and others and who has access to it. A copy can be accessed via the School Office.

CCTV imaging is collected, retained, and shared in accordance with the Information Commissioner's Office (ICO) code of practice.

Why we share information.

We share information:

- to safeguard and protect pupils and other vulnerable individuals in accordance with our Safeguarding and Child Protection policies and the Keeping Children Safe in Education Regulations and the Hampshire Safeguarding Children Partnership regulations to protect pupils and other vulnerable individuals for harm including sexual, emotional and physical abuse, neglect, exploitation, radicalisation and criminalisation, forced marriage and FGM.
- to ensure pupils with medical needs are properly supported and their needs met.

- to enable us to access funding and other support to enable pupils to access school, learning and the curriculum in accordance with our equalities' obligations.
- to enable us to provide services to our pupils (such as meals), before and after school clubs, co-curricular activities, and events/trips
- to enable us to provide appropriate and properly protected IT services to pupils.
- to enable us to manage our school budget and plan appropriately.
- to enable us to properly monitor and assess the effectiveness of the teaching and learning in the school.
- to celebrate the achievements of our pupils
- to ensure that receiving schools can support and provide for the needs of pupils leaving our school.
- to comply with our equalities' obligations
- to comply with our obligations to account for and monitor the impact of Pupil Premium and Sports funding.

Who do we share pupil information with?

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

Where it is legally required, necessary or permissible we may share personal information about pupils with:

- Schools that the pupils attend after leaving us.
- Schools, other educational settings, and other professionals who are providing educational, behavioural, and/or welfare support to our pupils.
- Individual pupils' families and/or representatives
- Our local authority (*Hampshire County Council (HCC)* - to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions)
- Financial organisations linked to HCC and our auditors from HCC.
- the Department for Education (DfE) on a statutory basis
- Ofsted
- External agencies where we have a safeguarding and/or child protection concern.
- the Police, courts, and tribunals
- Health Authorities
- Professional advisors and consultants
- Suppliers and service providers who provide services to you such as Tucasi, Timetable Rock Stars, Hampshire Catering
- Anonymised information on entitlement to Pupil Premium, SEND support/ECHP, assessment, progress, attendance and behaviour, with Governors, Ofsted Inspectors, and other education inspectors/advisers.
- Survey and research organisations.
- Professional bodies
- Third party providers of co-curricular activities both on and off-site

- Photographic material is used on our website and school publicity material in accordance with appropriate consent forms.

We share pupils' 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 pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. 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.

We are required by law to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice, or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data.

Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required.
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with 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>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Your Rights

Requesting access to your personal data

Under data protection legislation, individuals have a right to make “a **subject access request**” to gain access to information about them that we hold.

Parents/carers can make a request to access 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 a 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 such as assessment data and setting in a subject.
- 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.

If you would like to make a request, please contact our data protection officer.

Parents/carers also have a legal right to access their child's **educational record**. To request access, please contact the Headteacher at Cherrywood Community Primary School.

Other Rights

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

- object to processing of personal data that is likely to cause, or is causing, damage or distress.
- prevent processing for the purpose of direct marketing.
- object to decisions being taken by automated means (a computer or machine, rather than by a person)
- in certain circumstances, have inaccurate personal data rectified, blocked, erased, or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

To exercise any of these rights, please contact our data protection officer.

Complaints

We take complaints about our collection and use of personal information very seriously. If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance. To make a complaint contact our data protection officer.

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

- Report a concern online at <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 would like to discuss anything in this privacy notice, please contact:

Mrs. T. Gray, Data Protection Officer via the school office: Cherrywood Community Primary School, Mayfield Road, Farnborough, Hants, GU14 8HL. Tel: 01252 547896.
adminoffice@cherrywood.hants.sch.uk

Appendix 2: Privacy Notice - Parents and Carers

(How we use parent/carer/familial information)

The purpose of this Privacy Notice is to explain why we collect information, what information we collect, and how/why we might share it.

Please read this in conjunction with Privacy Notice (How we use Pupil Information) and our Data Protection Policy.

The categories of personal information that we collect, hold and share include:

- Personal information of parents/carers and other family members with parental responsibilities/emergency contact roles (such as name, address, telephone numbers, email details, special contact information/restrictions, names of siblings/other significant relationships where appropriate/necessary, car registration numbers)
- Special category data including characteristics such as ethnicity, language, nationality.
- Entitlement to apply for free school meals.
- Welfare, safeguarding and child protection information where this is relevant to, impacts on and/or is otherwise necessary to protect and support the pupil.
- Communications with parents/families
- Records of payments made/due to the school in relation to co-curricular activities (where payable), meals and other supplies.
- CCTV images/records captured in school or on school-based CCTV cameras.
- Photographic records of school events in which parents/others may appear.

Why do we collect, use, and share personal information?

We collect and use personal information to:

- Enable us to communicate effectively with parents/carers and ensure we comply with any contact restrictions.
- Access parents/those with parental responsibilities in the event of an emergency
- Provide appropriate pastoral care/support to pupils and their families.
- Safeguard and care for the pupils and other vulnerable individuals.
- Allow the school to access support (both practical and financial) for pupils and their families.
- Allow the school to plan for and appropriately support the welfare, health, emotional and social, as well as educational needs of pupils and families.
- Access health and social care support for pupils and families
- Monitor pupil attendance and behaviour.
- Allow school to provide and/or support access to sporting, cultural and other co-curricular activities/experiences to pupils.
- Ensure entitlement to free school meals.
- Allow the school to plan for and monitor access to and usage of Breakfast Club
- Allow the school to plan and monitor access to and usage of clubs/co-curricular activities.
- Allow the school to collect and monitor payments for school trips, lunches, and other income due to the school.
- Allow the school to communicate with parents, carers, and other stakeholders.
- Enable the school to meet its equalities and accessibility obligations.
- Record and celebrate the achievements of pupils and the school (*photos/videos*)
- Protect the individuals working in and/or visiting the school and the integrity of the premises and school assets (*CCTV*)
- Allow Governors to carry out their statutory duties.
- Assess the quality of our services and how well our school is doing.
- Assess and monitor the effectiveness of our school strategic plans.
- Statistical forecasting and planning including income.
- Allow the school to comply with its obligations to provide information to the local education and other education authorities/bodies.

- Comply with the law regarding data sharing.

The lawful basis for collecting and using personal and other information.

We only collect and use pupil personal information when the law allows us to do so.

The General Data Protection Regulation allows us to collect and use personal and other information where:

- We are complying with a legal requirement,
- Processing is necessary to protect the vital interests of a data subject or another person,
- where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and
- It is in the substantial public interest to do so.

Less commonly, we may also collect, hold, and use personal data where we have obtained consent to use it in a certain way.

Where we have obtained consent to use your personal information, 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.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children's Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

Some of the reasons listed above for collecting and using parent/carer/family personal information overlap, and there may be several grounds which justify our use of this data.

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Storing personal data

We hold personal data relating to parents/carers and families of pupils while the pupil is attending Cherrywood Community Primary School (where there are other family members in the school and the information is also relevant to them, it will be retained while these other pupils remain in the school). We may also keep it beyond the attendance of the pupil(s) at the school if this is necessary to comply with our legal obligations. Records containing personal information are securely stored and access to them is limited. Our Retention Schedule sets out how long we keep information on pupils, their parents/carers/family and who has access to it. A copy can be accessed via the School Office.

CCTV imaging is collected, retained and shared in accordance with the Information Commissioner's Office (ICO) code of practice.

Who do we share parents' information with?

We do not share personal information on our pupils' parents/carers or their families with anyone without consent unless the law or our policies allow us to do so.

Where it is legally required, necessary or permissible we may share personal information about parents/carers or families with:

- Schools that pupils attend after leaving us.
- Schools, other educational settings, and professionals who are working with/providing educational, behavioural, welfare or other support to the pupil/family/parent/carer.
- Health, welfare, and social care organisations
- External safeguarding and/or child protection agencies
- the Police, courts, and tribunals
- Professional advisors and consultants
- Survey or research organisations (anonymised)

Your Rights

Requesting access to your personal data

Under data protection legislation individuals have the right to make a **“subject access request”** to gain access to information about them that we hold. Parents/carers may make a request to access 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.

If you make a subject access request (in your own right or on behalf of your child), and we 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 such as assessment data and setting in a subject.
- 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.

If you would like to make a request, please contact our data protection officer.

Parents and carers also have a legal right to access to their child’s **educational record**. To request access, please contact the Headteacher at Cherrywood Community Primary School.

Other Rights

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

- object to processing of personal data that is likely to cause, or is causing, damage or distress.
- prevent processing for the purpose of direct marketing.
- object to decisions being taken by automated means (computer or machine, rather than by a person)

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

To exercise any of these rights, please contact our data protection officer.

Complaints

We take complaints about our collection and use of personal information very seriously. If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance. TO make a complaint contact our data protection officer.

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

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

Contact us:

If you would like to discuss anything in this privacy notice, please contact:

Mrs. T. Gray, Data Protection Officer via the school office: Cherrywood Community Primary School, Mayfield Road, Farnborough, Hants, GU14 8HL. Tel: 01252 547896.
adminoffice@cherrywood.hants.sch.uk

Appendix 3: Privacy Notice School Workforce

(How we use School workforce information)

The purpose of this Privacy Notice is to explain why we collect information, what information we collect, and how/why we might share it.

Please read this in conjunction with our Data Protection Policy.

The categories of school workforce personal information that we collect, hold and share include:

- Personal Information (such as name, address and other contact details, teacher number, banking details, driver's licence and passport information, emergency contacts, car registration numbers, national insurance number)
- Special categories of data including characteristics information such as gender, age, ethnicity, nationality, marital status, trade union membership
- Contract information such as start dates, hours worked, post, roles, and salary information.
- Qualifications/Clearances (such as academic qualifications, right to work, right to teach, DBS clearances)
- Safeguarding and child protection related information

- Performance management information including capabilities and grievances information.
- Pay related information.
- Health and well-being information
- Attendance/work absence information (such as number of absences and reasons)
- Training records
- Job application information (including references)
- Photographic and similar records (relating to workforce participation in teaching and learning activities/school events and trips, and the like)
- CCTV images and records captured on school premises or recorded from school premises.

Why do we collect and use personal information?

We collect and use school workforce personal information to:

- Support pupil learning.
- Safeguard all vulnerable stakeholders in the school.
- Administer employment contracts.
- Enable individuals to be paid.
- Enable the effective performance management of staff.
- Assess and monitor the quality of teaching and learning.
- Plan and administer staff development and training.
- Monitor and support staff well-being/health needs.
- Administer the deployment of volunteers within the school and monitor impact.
- Maintain records evidencing qualifications and completion of courses etc. which are relevant to /required to enable individuals and/or school to comply with statutory obligations and/or support pupil learning.
- Meet equalities legislation obligations.
- Ensure accessibility for all stakeholders.
- Enable the school workforce to have access to and maintain access to appropriate online/IT facilities.
- Allow the school to provide lunch services to staff.
- Allow the school to plan for and monitor provision of Breakfast Club
- Allow the school to plan and monitor provision of clubs/co-curricular activities.
- Provide evidence of/record and celebrate the achievements of pupils and the school.
- Protect the individuals working in and/or visiting the school and the integrity of the premises and school assets.
- Enable the Governing Body to carry out their statutory duties.
- Support school improvement.
- Assess the quality of our services and how well our school is doing.
- Assess and monitor the effectiveness of our school strategic plans.
- Statistical forecasting and planning including income.
- Enable the development of a comprehensive picture of the workforce and how it is deployed.
- Inform the development of recruitment and retention policies.
- To allow the school to comply with its obligations to provide information to the local education and other education authorities/bodies.
- To comply with the law regarding data sharing

Our lawful basis for collecting and using personal and other information about the school workforce.

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 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 - for example, where:
 - Additional resources are required to ensure your safety and adapted work environment.

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 personal information

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

We will inform you whether you are required to provide certain personal information to us (and if so, what the possible consequences are of not complying), or if you have a choice in this.

How we store your personal data

We create and maintain an employment file for each member of the school workforce. The information contained in this file is kept secure and is only used for purposes related to your employment. It can only be accessed by the Headteacher, DSL/DDSL (if necessary), and the Business Manager. Contact details are entered into SIMS by the Administration Officer.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Retention Schedule.

Any member of staff may request access to his or her files upon written request from the headteacher. Access to the file is under supervision by either the Headteacher or the Data Protection Officer.

CCTV imaging is collected, retained and shared in accordance with the Information Commissioner's Office (ICO) code of practice.

Data Sharing

We do not share information about you with any third party without your consent unless the law or our policies allow us to do so.

Where it is legally required, or necessary we may share personal information about you with:

- Our local authority
-
-

- The Department for Education - this data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.
- Your family or named representatives.
- Suppliers and service providers - to enable them to provide the service we have contracted them for, such as payroll, occupational health, personnel/HR services.
- IT providers with whom we have contracted to provide IT resources for use by the workforce in the execution of their school roles.
- Trade union and associations
- External professional advisers and consultants
- Training providers
- Ofsted inspectors (generally anonymised)
- Governors to enable them to carry out their statutory obligations (including for Pay Committee (anonymised), safeguarding and financial audits, and grievance/appeal committees)
- External agencies concerned with safeguarding and child protection.
- Potential employers in response to a reference request
- Employment and recruitment agencies
- The Police, courts, and tribunals
- Security organisations
- Professional bodies
- Our HCC auditors
- Survey and research organisations.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements:

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). 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>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

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>

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.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress.
- prevent processing for the purpose of direct marketing.
- object to decisions being taken by automated means.

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

To exercise any of these rights, please contact our data protection officer.

Complaints

We take 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 us in the first instance.

To make a complaint, please contact our data protection officer - Mrs. T. Gray.

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

- Report a concern online at <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 would like to discuss anything in this privacy notice, please contact:

Data Protection Officer, Mrs. T. Gray, via the school office: Cherrywood Community Primary School, Mayfield Road, Farnborough, Hants, GU14 8HL. Tel: 01252 547896.
adminoffice@cherrywood.hants.sch.uk

Appendix 4: Privacy Notice - Governors

(How we use Governor information)

The purpose of this Privacy Notice is to explain why we collect information, what information we collect, and how/why we might share it.

Please read this in conjunction with our Data Protection Policy.

The categories of governor personal information that we collect, hold and share include:

- Personal Information (such as name, address and other contact details, driver's licence and passport information, car registration numbers)
- Special categories of data including characteristics information such as gender, age, ethnicity, nationality, marital status
- Qualifications/Clearances (such as DBS clearances)
- Safeguarding and child protection related information

- Register of Interests
- Attendance information
- Training records
- Governor application information
- Minutes of Meetings
- Governor Monitoring Reports
- Roles and Responsibilities information
- Photographic and similar records (relating to governor participation in school activities/school events and trips, and the like)
- CCTV images and records captured on school premises or recorded from school premises.

Why do we collect and use personal information?

We collect and use Governor personal information to:

- Enable effective and safe recruitment.
- Allow Governors to carry out their statutory duties.
- Permit accessibility for all stakeholders.
- Safeguard all vulnerable stakeholders in the school.
- Allow the School and the Governing body to plan and administer Governor development and training.
- Plan and evaluate the work of the Governing body.
- Record and evaluate School strategic plans.
- Enable effective planning and monitoring of the School's budget and other resources.
- Maintain records of Governor monitoring
- Record the business of the Governing body.
- Monitor and avoid potential conflicts of interest.
- Celebrate the work of the school, staff, and pupils.
- Ensure the security of the school site, premises, and assets.
- Allow the school to comply with its obligations to provide information to the local education and other education authorities and/or governmental bodies (such as Governor attendance at meetings)
- Comply with the law regarding data sharing.

Our lawful basis for collecting and using personal and other information about Governors.

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

- 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 - for example, where:
 - Additional resources are required to ensure your safety and adapted work environment.

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 personal information

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

We will inform you whether you are required to provide certain personal information to us (and if so, what the possible consequences are of not complying), or if you have a choice in this.

How we store your personal data

Governor personal information acquired as part of the DBS clearance process is recorded in the electronic and encrypted Single Central Register which is accessible only to the Designated Safeguarding Lead/Headteacher or Deputy Designated Safeguarding Leads (if necessary), and the School Business Manager. We do not retain copies of DBS certificates, but copies of documents produced to support this clearance process are retained in a Governor file, which is kept secure and only used for the purposes of checking DBS clearances and safeguarding matters.

Other personal information is held, deleted, and shared in accordance with our Retention Schedule, a copy of which can be accessed via the School Office.

CCTV imaging is collected, retained and shared in accordance with the Information Commissioner's Office (ICO) code of practice.

Data Sharing

We do not share information about you with any third party without your consent unless the law or our policies allow us to do so.

Where it is legally required, or necessary we may share personal information about you with:

- Our local authority
- The Department for Education - this data sharing underpins Governor workforce policy monitoring, evaluation, and links to the assessment of the quality of leadership and educational attainment.
- IT providers with whom we have contracted to provide IT resources for use by the workforce in the execution of their governor roles.
- External professional advisers and consultants
- Training providers
- Ofsted inspectors
- External agencies concerned with safeguarding and child protection.
- The Police, courts, and tribunals
- Security organisations
- Professional bodies
- Our HCC auditors
- Survey and research organisations.

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.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress.
- prevent processing for the purpose of direct marketing.
- object to decisions being taken by automated means.
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

To exercise any of these rights, please contact our data protection officer.

Complaints

We take 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 us in the first instance.

To make a complaint, please contact our data protection officer - Mrs. T. Gray.

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

- Report a concern online at <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 would like to discuss anything in this privacy notice, please contact:

Data Protection Officer, Mrs. T. Gray via the school office: Cherrywood Community Primary School, Mayfield Road, Farnborough, Hants, GU14 8HL. Tel: 01252 547896.
adminoffice@cherrywood.hants.sch.uk

Appendix 5: Privacy Notice - Visitors, contractors and suppliers

(How we use Visitor, Contractors and Suppliers information)

The purpose of this Privacy Notice is to explain why we collect information, what information we collect, and how/why we might share it.

Please read this in conjunction with our Data Protection Policy.

The categories of visitor, contractor, and supplier personal information that we collect, hold and share include:

- Personal Information (such as name, address and other contact details, car registration numbers)
- Company details
- Contract information/Terms and Conditions of Business
- Qualifications/Clearances (such as DBS clearances, insurance information, professional qualifications if relevant to the service provided)
- Safeguarding and child protection related information
- Payment related information (such as banking and VAT details)
- CCTV images and records captured on school premises or recorded from school premises.

Why do we collect and use personal information?

We collect and use visitor, contractor, and supplier personal information to:

- Safeguard all vulnerable stakeholders in the school.
- Administer contracts including making payments.
- Ensure accessibility for all stakeholders.
- Protect the individuals working in and/or visiting the school and the integrity of the premises and school assets.
- Enable the Governing Body to carry out their statutory duties.
- Assess the quality of our services and how well our school is doing.
- Assess and monitor the effectiveness of our school strategic plans.
- Statistical forecasting and planning including income.
- Comply with the law regarding data sharing.

Our lawful basis for collecting and using personal and other information about visitors, contractors and suppliers.

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, for example, where
 - Additional resources are required to ensure your safety and adapted work environment.

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 personal information

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

We will inform you whether you are required to provide certain personal information to us (and if so, what the possible consequences are of not complying), or if you have a choice in this.

How we store your personal data

We retain personal data about visitors, contractors and suppliers for so long as they continue to have a relationship with the school (including for any post-work/contract warranty period) and/or for so long as we are legally required to do so. Personal information is held and deleted (and shared) in accordance with our Retention Schedule, a copy of which can be accessed via the School Office.

CCTV imaging is collected, retained and shared in accordance with the Information Commissioner's Office (ICO) code of practice.

Data Sharing

We do not share information about you with any third party without your consent unless the law or our policies allow us to do so.

Where it is legally required, or necessary we may share personal information about you with:

- Our local authority including the finance department and payment teams to facilitate payment (including via the IBC payment and shared services system)
- Governors to enable them to carry out their statutory obligations.
- External agencies concerned with safeguarding and child protection.
- Potential employers in response to a reference request

- The Police, courts, and tribunals
- Security organisations
- Professional bodies
- Our HCC auditors
- Survey and research organisations.

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.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress.
- prevent processing for the purpose of direct marketing.
- object to decisions being taken by automated means.
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

To exercise any of these rights, please contact our data protection officer.

Complaints

We take 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 us in the first instance.

To make a complaint, please contact our data protection officer - Mrs. T. Gray.

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

- Report a concern online at <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 would like to discuss anything in this privacy notice, please contact:

Data Protection Officer, Mrs. T. Gray. via the school office: Cherrywood Community Primary School, Mayfield Road, Farnborough, Hants, GU14 8HL. Tel: 01252 547896.
adminoffice@cherrywood.hants.sch.uk

Appendix 6: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been.
 - Made available to unauthorised people.
- The DPO will alert the headteacher and the chair of governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud.
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation.
 - Loss of confidentiality

- Any other significant economic or social disadvantage to the individual(s) concerned.

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

- The DPO will document the decision 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 staff/student's personal files.
- Where the ICO must be notified, the DPO will do this via the ICO Website (ico.org.uk) or telephone 0303 123 1113 within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned.
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school shared drive in an access limited folder and a copy will also be placed on staff/student personal file.

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

Actions to minimise the impact of data breaches.

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

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

Other types of breach that may be included in the definition of data breach include:

- *Details of pupil premium interventions for named children being published on the school website.*
- *Non-anonymised student exam results (without consent) or staff pay information being shared with governors.*
- *A school laptop containing non-encrypted sensitive personal data being stolen, lost or hacked.*
- *Other online educational systems that have been hacked and personal details disclosed such as Timetable Rockstars etc.*
- *Non-anonymised student level data that contains personal data such as dates of birth, genre, SEND etc. has been lost, stolen or used by a third party not employed in the school.*