The Canons C of E PRIMARY SCHOOL

Information Security Policy
GDPR
2024

Signed Head Teacher

Signed Chair of Governors

Policy Approved Date	**June 2024**
Policy Review Date	**June 2027**

Y:\POLICIES & PROCEDURES\a THE CANONS\Adopted\GDPR\GDPR Policies\Information Security Policy\Information Security Policy 2024.docx

Information Security Policy

Contents

Apendices1

1. Scope

This Policy applies to:

- All members of staff, governors ; “Staff” includes all employees, locum staff, volunteers, work experience and any other individuals working for The Canons CE Primary School on a contractual basis.

The Importance of this Policy:

- This information Security Policy lets you know what your Information Security responsibilities are at The Canons CE Primary School everyone has a role to play and it’s vital you understand yours.

The Objective of this Policy is to:

- Inform staff, governors and protect The Canons CE Primary School from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff, governors of The Canons CE Primary School complying with this policy.

2. Key Principles

The Canons CE Primary School **has adopted the following six principles to underpin its Information Security Policy:**

All Personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

3. Creating, storing and managing information

The Canons CE Primary School **has adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.**

The purpose of this section is to establish The Canons CE Primary School's re**quirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals**.

3.1 Paper information

● Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.

● Confidential documents must not be left on display or unsupervised.

● Store confidential information in locked cabinets, returning them to these cabinets when not required.

● Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.

● Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.

● Spoiled photocopies and prints may still be confidential. Do not put them straight into the waste paper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies. (Aveena Waste Disposal)

● Dispose of confidential paper by shredding or put in a confidential waste bag and follow confidential waste disposal procedure. Do not dispose of confidential waste in a waste paper bin or anywhere else.

● Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

3.2 Electronic information

● All confidential information must be stored on The Canons CE Primary School approved electronic devices or systems with access controlled/restricted, e.g. the The Canons CE Primary School network,.

● Confidential information must not be stored on local unencrypted hard drives.

● If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by The Canons CE Primary School

● PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g. through windows or while waiting in public areas.

● Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below).

● Individual user id/passwords must not be shared with anyone, including other staff members and governors, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on The Canons CE Primary School network using your network id.

● Passwords must not be written down and left with any equipment or accessible by anyone else.

● Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already.

● Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.

● If you find you have access to confidential information that you believe should be restricted, you should notify Mrs Fallon Head Teacher or Mrs Thomas School Business Manager immediately.

4. Receiving, sending and sharing information

4.1 Post – receiving and sending

● Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays'.

● Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.

● If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package.

● Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address.

● When using a mailshot or multiple mailings, have a procedure in place to check you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.

● Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.

● Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.

● If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

4.2 Email and Other Electronic Communications (e.g. text messages) – receiving and sending

● The Canons CE Primary School does not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.

● If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.

● Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.

● If sending to a list/group of parents or others, send using ‘blind copy’ (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.

● Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;

a) you are using an encrypted email service provided by The Canons CE Primary School or

b) the information is encrypted / password protected in an attachment, or

c) you are sending to an approved The Canons CE Primary School email address, e.g. a school welearn email address, or Warwickshire.gov

d) you are sending to an e-mail address which utilises the same server – for schools which use the ‘welearn’ e-mail system this includes all other schools with this system as well as Warwickshire County Council.

● Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as The Canons CE Primary School records.

● The Canons CE Primary School Confidential email must not be forwarded to your own personal email account for private use.

4.3 Telephone calls

● Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.

● If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.

● If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.

● If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.

● Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.

4.4 Conversations

Staff should remember that even though they may be on The Canons CE Primary School premises there may be pupils and visitors around.

● When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.

● Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.

● Always consider your surroundings and the proximity of others who may be able to hear in public places.

4.5 Information sharing/processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

1. If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf of The Canons CE Primary School or has sole or joint responsibilities for the personal data with The Canons CE Primary School. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them.

2. If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information

agreement exists and what obligations that might place on them, it should be clarified with their manager.

5. Working Away from School

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the school, at home and use of own devices to access personal and confidential information.

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in school, on the phone, at home, en route to or from school or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in clear folder.

- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.

- Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away.

- Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information.

- Use of Laptops: Only school issued devices may be used. Do not write down passwords/pin numbers. You must not use the ‘remember me’ option to save user and password details on your device when accessing The Canons CE Primary School system. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from ‘downloads’. If files are not accessed directly (e.g. Google drive format files), then all confidential files must stored and accessed locally via The Canons CE Primary School approved encrypted media.

● Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Don't leave any of The Canons CE Primary School equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal. Use strong security on a home WiFi connection.

6. Premises security

● All staff must wear their ID badge on school premises and report losses or thefts immediately to their line manager.

● Make sure that all visitors sign in and out at all times and disclose who they are coming to see. Visitors should be supervised at all times and display a visitor/contractor ID badge.

● Staff should be encouraged to challenge anyone in the school if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing an ID badge.

● Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary.

● Managers should ensure that all paper based records and any records held on computers are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced

● Parents and others who do not want to discuss their private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere.

7. Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across The Canons CE Primary School **. Portable media devices include, but are not limited to USB sticks or memory cards.**

● Connection of The Canons CE Primary School -supplied removable media devices to the The Canons CE Primary School computing infrastructure is only permitted for the purpose of reading files from the device; The Canons CE Primary School files must not be written to a non The Canons CE Primary School -supplied device.

● Staff must not alter or disable any controls applied to any computing device by The Canons CE Primary School IT Service as part of the deployment of a removable media device.

● Removable media devices must not be used for the primary long-term storage of The Canons CE Primary School information.

● All information classified as 'The Canons CE Primary School Confidential' or 'personal' that is stored on a removable media device must be encrypted.

● Passwords applied to encrypted devices must conform to the minimum standard required stated in section 3.2 Electronic Information of this Policy.

8. Anti-Malware

The purpose of this section is to establish requirements, which must be met by all devices within The Canons CE Primary School' **s computing infrastructure, to protect the confidentiality, integrity and availability of** The Canons CE Primary School **software and information assets from the effects of malware.**

● Unless undertaken by or following instruction from IT support staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices.

● The intentional introduction of viruses to The Canons CE Primary School 's computing infrastructure will be regarded as a serious disciplinary matter.

● Only software that has been authorised by The Canons CE Primary School can be installed upon The Canons CE Primary School systems.

● Each member of staff is responsible for immediately reporting any abnormal behaviour of The Canons CE Primary School computing systems to the IT Service Desk/Anthony Manton - IT Consultant

● Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.

9. Access Control

● Access to information shall be restricted to users who have an authorised need to access the information.

● Users of information will have no more access privileges than necessary to be able to fulfil their role.

● All requests for access to The Canons CE Primary School computer systems must be via a formal request to the Senior Leadership Team.

● The Canons CE Primary School reserves the right to revoke access to any or all of its computer systems at any time.

● Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.

● Users must not allow anyone else to use their account, or use their computers while logged in with their account.

● Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.

● Users should not leave workstations or devices in 'sleep mode' for convenience.

10. Monitoring System Access and Use

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of The Canons CE Primary School 's information and information systems.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The Canons CE Primary School will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

11. Potential breaches of security or confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it immediately to a member of the Senior Leadership Team immediately.

For losses of equipment or if you believe your email or the network may be at risk, contact the School Business Manager immediately on 024 76 312220.

If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.

Use The Canons CE Primary School procedure to report and record incidents. If you are aware of a potential incident email to: head3302@welearn365.com or Thomas.d4@welearn365.com as soon as possible and in any event within 4 hours.

Appendix 1 - Security obligations under the GDPR

Although the security of personal data has been a legal obligation for data controllers under the Data Protection Act 1998, the GDPR reinforces the existing provisions and also extends this responsibility directly to those individuals who actually process the data.

Security of data processing

The GDPR requires personal data to be processed in a manner that ensures its security. This is commonly known as the GDPR's 'security principle'.

The security principle means that you must take measures to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

The GDPR requires organisations to secure information assess risk and put appropriate security measures in place.

What do security measures need to protect?

The security of personal data goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable so that if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability'. The controller and processor must also take steps to ensure that any person acting under their authority and having access to personal data, does not process the data except on instructions from the controller (unless otherwise required by law).

What level of security is required?

The GDPR requires you to have 'appropriate' security measures in place.

The GDPR does not dictate which security measures you should have in place as no 'one size fits all'.

What's 'appropriate' depends on your individual circumstances, the processing you're undertaking and the risks presented by the processing. When deciding which security measures are 'appropriate' you will also take into account the costs of implementation and the nature, scope, context and purpose of your processing.

GDPR relates the risk to the measures taken in order to protect the rights and freedoms of individuals about whom the information relates.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf: for example, an external organisation who processes personal data (such as pupil photographs) on your behalf. (We shall be providing you with guidance on data processors acting on your behalf in a future bulletin).

What security measures need to be considered?

'Appropriate' technical and organisational security measures for the protection of personal data should be implemented to ensure data security.

- **Organisational measures –** Examples include carrying out an information risk assessment; encouraging and creating a culture of security awareness; introducing an information security policy which demonstrates the steps you take to ensure data security; ensuring premises or equipment are protected against unauthorised access; having arrangements in place to protect and recover personal data you hold; and carrying out periodical checks to ensure security measures are appropriate and up to date.
- **Technical measures –**These include both physical and IT/computer security. Examples of physical security include: door locks in areas where personal data is stored; protecting your premises by alarms, security lighting or CCTV; procedures you have in place to ensure IT equipment is secure; and how you dispose of paper and electronic waste (i.e. old computers). Examples of IT/computer security include: taking steps to ensure your network and systems are secure; having access controls in place on your network and systems; ensuring IT/computer devices are secure (i.e. USB sticks and laptops).

Whatever you do, you should remember the following: your security measures need to be appropriate to the size and use of your network and information systems; you should consider the costs of implementation; your security must be appropriate to your business practices (For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security); and your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

Pseudonymisation and encryption

The GDPR provides specific suggestions for what types of security measures might be considered “appropriate to the risk”. These include the pseudonymisation and encryption of personal data.

Pseudonymisation (removing personal identifiers) and encryption (encoding it – by use of password protection, for example) are recommended by the ICO as tools for safeguarding information. However both of these can be implemented at relatively low cost and with minimal difficulty. The ICO has for a number of years considered encryption to be an appropriate technical measure – this position has not altered under the GDPR.

‘Confidentiality, integrity and availability’

These are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

What about your staff?

You are required to take steps to ensure that any person acting under your authority with access to personal data, does not process the data except as you have instructed them to do so (unless otherwise required by law).

It’s therefore important that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, including:

●responsibilities under the GDPR;

●staff responsibilities for protecting personal data; and

●any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or spam).

We will be providing materials to help you do this.

Are your security measures effective?

You should have a process for regularly testing, assessing and evaluating the effectiveness of any security measures you put in place.

It does not specify the type of testing which should be carried out or how regularly the testing should occur. These will depend on your organisation and the personal data you are processing.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

Appendix 2 - Advice - Lawful Basis for Processing

This might well be the most important piece of advice you read during the GDPR implementation period. We would ask that you read it in full because the implications are very significant for what you can do as a school with personal data. If you have any questions about the advice, particularly in relation to what lawful reason can be used for processing, then please contact us.

In order to process personal data, you **must** have a lawful basis. This is not a new concept, it is a requirement that also exists in the Data Protection Act 1998. GDPR does however require you to be more transparent about the lawful basis you are relying upon for processing and also, crucially, removes one of the more commonly used lawful bases from the suite available to public sector bodies such as schools.

Certain types of personal information, called '**special categories**', have further requirements which must be complied with in addition to the rules for normal personal information, and we will deal with these at the end of this advice note – please make sure that you read this section as well.

The six lawful reasons for processing the majority of personal data are:

1. The individual has given clear consent for you to process their personal data for a specific purpose (**Consent**)
2. The processing is necessary for a contract you have with an individual or because they have asked you to take specific steps before entering into a contract (**Contract**)
3. The processing is necessary for you to comply with the law (**Legal Obligation**)
4. The processing is necessary to protect someone's life (**Vital Interests**)
5. The processing is necessary to perform a task in the public interest or your official functions, and the task or function has a clear basis in law (**Public Task**).
6. The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (**Legitimate Interests**)

GDPR has changed the Data Protection Act position so that the **'Legitimate Interests' reason cannot be used by public authorities, including schools, as a reason to process information in performance of their tasks**.

The loss of '**Legitimate Interests**' means that there are in reality only five lawful reasons available to schools. This advice paper explains which of these is suitable in which circumstances, and will enable you to both complete your data mapping, and also to ensure that appropriate Privacy Notices can be drawn up.

You will notice that four of the five lawful reasons available to you include the word "**Necessary**". In the legal sense "Necessary" does not mean that processing always has to be essential. The lawful basis will not apply if you can reasonably achieve the

purpose by some other less intrusive means. It is not enough to assert that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

The GDPR now places an additional requirement on data controllers to provide individuals with information about the lawful basis (reason) which is being relied upon to process information and details of this will need to be set out in your privacy notice.

Consent

This is often described as being a 'default' ground, in that you can do whatever you wish with a person's personal information, so long as they have consented to it. We have already provided you with advice on obtaining consent, and in particular on ensuring that it is provided by a 'clear affirmative act', meaning that 'implied consent' is not lawful for these purposes and that written evidence of consent having been given should be held by the school.

Our advice would be that 'Consent' should not be regarded by you as being the lawful basis for processing personal information if another lawful reason is available because:

- you need to ensure that you have a record of the clear affirmative consent for use of personal information in the particular circumstances; and
- parents (and potentially pupils) have the ability to withdraw consent at any time and for any reason.

It therefore makes it difficult to plan for any long term processing with confidence.

We would therefore recommend that you only seek consent for the processing of personal information if no other lawful reason is available. This advice note should help you decide whether another reason can be used.

Contract

Personal information can be processed if it is necessary in order to comply with a contract you have with the person concerned. Please note however that you do not have legally binding contracts with pupils or parents (Home School Agreements do not meet the legal definition of a contract) and as such this lawful reason cannot be used in relation to any processing of their personal data.

This lawful reason may however be used in relation to information about members of staff which needs to be processed for reasons related to the contract, rather than for statutory purposes. This might, for example, include processing personal information to give staff access to certain benefits to which they are entitled as a result of their employment contract.

Legal Obligation

Much of the data sharing and processing that you carry out will be as a result of legal obligations that schools are subject to. This advice note is accompanied by a table of legal obligations which schools are required to comply with under education legislation. This should help you to understand which specific legal obligations you are complying with at any particular time. You should find this helpful when completing both the data mapping task and, in time, your Privacy Notices and Data Protection Policy.

We have kept this table deliberately short in order for it to not to be too confusing, and to cover what we feel are the vast majority of legal requirements you have to share information with others, as well as the requirement to hold an educational record, which includes all information that the school should need to have about a pupil. If you think that a legal obligation allows, or requires, you to process particular information but does not appear on our list then please let us know and we can advise you further. You should not use 'Legal Obligation' as your justification for processing unless you can identify the particular piece of legislation or other law which allows you to do so.

There are some circumstances where information sharing will not have a simple justification under GDPR, but where you are confident that a legal obligation does exist. In those circumstances we are happy to discuss with you what we feel is most appropriate.

The table of duties also includes the two sets of Regulations which govern Income Tax and National Insurance returns for staff, and these should therefore be included as the justification for sharing information with HMRC. Due to the complex nature of the legislation we would recommend just referring to the Regulations as a whole rather than to individual sections.

Please therefore look through your data mapping tool and, where legal obligations justify such tasks, complete with details of the legal obligations set out in the accompanying table.

Vital Interests

The 'Vital Interests' lawful reason is only to be used in an emergency, where a person's life is in danger. Appropriate circumstances might well therefore include the sharing of key information with paramedics, the police or the fire service where a risk of serious harm or death exists if information is not revealed. It may be worth having an appropriate line in your data mapping tool to take account of the need to share information in such circumstances.

Public Task

It is worth taking account of the fact that much of the work involved in educating children and young people is not actually set out directly in legislation. It is the day-to-day task of ensuring that children receive the education and support that they require, and which will inherently require information sharing and use between staff to ensure that pupils are properly supported. This constitutes a 'Public Task' because your job

as a school is to educate children, even though you will struggle to find a single piece of legislation which says this, and therefore internal processing and sharing which is necessary both to educate and safeguard your pupils is lawful.

You do need to note however that processing for 'Public Task' purposes must still be necessary. For example, it is not currently considered by the DPO Service that it would be appropriate or lawful for a school to justify the sharing of personal information with a web-based educational resource using the 'Public Task' lawful reason unless the use of such a resource was an educational requirement. In such circumstances it would be more appropriate to utilise 'Consent' as the lawful reason.

Special Categories

Personal information which reveals any of the following is classified as 'Special Category' information, and a separate set of rules governs whether this can be processed:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic and / or Biometric data
- Health information
- Information concerning a person's sex life or sexual orientation

It is likely that you do hold some of the above in relation to both pupils and staff members, for example some staff information concerning trade union status and health issues, as well as medical information about pupils.

In these circumstances you need to be able to demonstrate why the law allows you to hold/share the information (i.e. which one of the five legal reasons above applies) **and also** prove one of the following additional 'Lawful Reasons' apply.

There are ten 'Lawful Reasons' for holding and processing this information, but these are far more restrictive than in relation to general personal information referred to above.

Again, in order to process personal data, you **must** have a lawful basis (i.e. one of the five legal reasons above **and** one of the following Lawful Reasons must apply:

1) **Data Subject has given explicit consent**: In the same way as for other forms of personal data, you should ensure that this is provided by a 'clear affirmative act', meaning that 'implied consent' is not lawful for these purposes and that written evidence of consent having been given should be held by the school. Consent can be withdrawn at any time.
2) **Necessary for carrying out obligations and exercising specific rights in relation to employment and social security and social protection law:** This

can be used in relation to staff information if a legal obligation requires you, or a legal right enables you, to hold particular information, so long as this is necessary.

3) **Necessary to protect vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent**: This is similar to the 'Vital Interests' ground above, but can only be used where the person concerned is 'physically or legally incapable' of giving consent. Again, this can be used in emergency situations where a person's life is in danger and vital information needs to be given to health staff, police or fire crews, particularly in relation to health information relevant to emergency medical treatment.
4) **Processing carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim**: This is not available to schools and academies
5) **Processing relates to personal data which is manifestly made public by the data subject**: Being manifestly made public means that the person concerned has published this information publicly, either on the internet or for general public consumption – not just for use by a school. We would suggest that this is a ground that should not be relied upon by schools without expert advice.
6) **Necessary for establishing, exercising or defending legal claims**: Only to be used when receiving legal advice or in relation to legal proceedings.
7) **Necessary for reasons of substantial public interest**: This is highly unlikely to be suitable for use by schools or academies as it is intended for use to protect life or as a result of public interest investigations by the media, police, government or others.
8) **Necessary for preventive or occupational medicine**: This will be used by schools regularly in relation to assessment of employee working capacity, and also in some circumstances relating to pupils (in less serious cases than the 'Vital Interests' reason above, but there must still be a strong element of necessity for processing).
9) **Necessary for reasons of public interest in the area of public health**: This can be used if there are serious threats to health on a large scale, so is unlikely to be used in your data mapping as a regular processing issue.
10) **Necessary for archiving, historical research or statistical purposes in the public interest**: This is not suitable for schools or academies.