FERNHURST PRIMARY SCHOOL

Nurture | Explore | Achieve

Haslemere Road | Fernhurst | Surrey | GU27 3EA
Tel: 01428 653144 | www.fernhurst.w-sussex.sch.uk

Data Protection (GDPR) Policy

Created	May 2018
Responsible Committee	Curriculum & Standards
Ratified by Finance and Resources	June 2018
Next Review	Summer 2021

Data Protection Policy

The University of Chichester Academy Trust is a group of schools operating under a single legal entity. This policy therefore covers all aspects of the Trusts work including the activity of its schools.

The Trust collects and uses personal information, referred to in the General Data Protection Regulation (GDPR) as personal data, about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered to enable the provision of state funded education and its associated functions. The school is required by law to collect, use and share certain information in the public interest.

Purpose
This policy sets out how the Trust, including each if its schools, deals with personal information correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the Trust including each of its schools and whether it is held on paper or electronically.

What is Personal Information/data?
Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The Trust will adopt the six principles of the General Data Protection Regulations(GDPR) as well as a number of additional duties stated in the regulations that will be adhered to at all times:

1. Personal data will be processed lawfully, fairly and in a transparent manner

2. Personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes 3.)

3. Personal data collected will not be excessive and will be adequate, relevant and limited to what is necessary to the purposes for which it is processed;

4. Personal data will be accurate and kept up to date;

5. Personal data will be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

6. Personal data shall be processed in a manner that ensures the appropriate security of the person

Personal data will not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Protection Roles

The Trust has a **Data Protection Officer**, Helen Turner, who may be contacted at unicat@chi.ac.uk. She has the overall Responsibility for Data protection across the Trust and will be the link with the Information Commissioners Office on behalf of all of the schools in the Trust. Her name and contact details should be on each schools website.

The role of the Data Protection Officer is:

- to keep the Trust Data Protection Policy up to date at all times
- to provide templates and consent forms for all of the schools and the central Trust staff
- to provide data protection training to Data Champions
- to manage the data breach procedure
- to be the first point of contact with the Information Commissioner's Office
- to report on data protection matters to the Trust Board.

The Trust has also allocated a Trustee from the Trust Board to oversee this area of work to provide governance support to the Data Protection Officer and assurances to the Board that risks and issues are being appropriately managed.

Each school has a **Data Champion** who will keep the Data Protection Officer informed of any breaches in data control and will be the first point of contact within the school for parents and the local community.

The role of the Data Champion is:

- to keep the school's record of data (the database) up to date at all times
- to ensure that Data Impact Assessments are completed for any new type of data processing activity
- to ensure that a due diligence checklist is completed for all new third party data processors and that contracts are compliant with GDPR
- To ensure good GDPR awareness in the school and induction and ongoing training for all staff
- To report to the governing body on any issues which have arisen and the actions taken to resolve them.

Data Control within an individual school will be delegated to the Local Governing body who will have a General Duty of accountability for personal data that the individual school collects and receives for its purposes. Thus the Local Governing Body is the **Data Controller.**

Commitment
The Trust is committed to maintaining the principles and duties in the GDPR at all times.

In order to do this the school will:

- Inform individuals of the identity and contact details of the data champion who in most cases will be the Head teacher
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the contact details of the Data Champion in the school; this may or may not be the data controller.
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept

Most of the information above will be shared when a child joins the school and will be reviewed when needed but as a minimum on an annual basis.

- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual - or parent if the individual is under 13- and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

The school will provide information to staff and governors when they join the school and will also provide an update every September or more frequently if regulations change or issues emerge.

The Trust Data Protection Officer will advise, following an investigation, on whether a breach is a reportable incident and will report all reportable incidents to the ICO within 72 hours of the breach being reported.

The school Data Champion will report to the Local Governing Body of the school on a termly basis and is also the first point of contact in the school for any issues. The Local Governing Body has delegated responsibility to be the Data Controller of the personal data that the individual school collects and receives for these purposes. The Data Champion will inform the Chair of Governors and the Data Protection Officer immediately if there are any reportable incidents and will take immediate action on other issues.

The school will issue Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff when they join the school and they will also be available on the website. If these notices are reviewed or changed all parents/pupils (over 13) and staff will be notified. These notices summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be legitimately shared with in order to deliver the schools public duty. It also provides information about an individual's rights in respect of their personal data

Complaints
Complaints relating to the handling of personal information will be dealt with in the first instance in accordance with the school's complaints policy and will be overseen by the Data Champion and the Data Protection Officer and Chair of Governors will be notified immediately.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer and the Trust Board.

Contacts
If you have any enquires in relation to this policy, please contact the school's data champion in the first instance whose details are…… You may also contact the Trust's Data Protection Officer, Helen Turner, at unicat@chi.ac.uk or 01243 793500.

Key document details

Last Review	**May 2018**
Department/Owner	**Data Protection Officer**
Review Date	**May 2020**

The following annexes form part of the Data Protection Policy;

Annexe 1
Electronic Information Security Policy - schools

The information systems policy covers the use of ICT systems to support learning, the use of telephones, email and the internet by staff, and the use of online tools provided by the school. This policy consists of three sections:

1. **Acceptable use of ICT equipment**
2. **Use of telephones, email and internet by staff**
3. **Safe use of online resources**

1. Acceptable use of ICT Equipment

The Trust is committed to safeguarding all ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure is the responsibility of all staff.
The school encourages staff to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. The school encourages this use in a responsible and professional manner.
As a user of ICT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, you may be subject to disciplinary procedures.
Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.
Staff are advised of this policy during their induction and of the school's requirement for them to adhere to the conditions therein.
For the purposes of this policy the term "computing services" refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Staff who connect their own ICT to the School's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

- To ensure Trust schools are able to provide a high quality education supported by a well- protected ICT infrastructure
- To protect the school's networks and equipment
- To protect the school's data
- To protect the school and its employees from activities that might expose them to legal action from other parties

Guidelines Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the School.
Issuance and continued use of your User Account is conditional on your compliance with this policy. User IDs and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others or allow others to access or use their account once opened will be in breach of this policy.
Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be routinely changed and should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of school "computing services" should be for teaching and/or administrative purposes of the school. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use of the school's computing services must at all times comply with the law.
- Your use of the school's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such.
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by your IT provider for installation
- You must not use any peer-to-peer file sharing software
- You must not use any IRC or messenger software unless expressly authorized to do so for work related purposes
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the school's facilities, unless specifically related to school activities
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Head teacher

Data Security

The school holds a variety of sensitive data including personal information about pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

You should only take a copy of data outside the school's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, mobile devices or into emails. If you do need to take data outside the school, this should only be with the authorisation of the Head teacher. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the School, and these should always be used in preference to taking data off-site.

The school's IT provider will be able to advise further.

Anti-Virus and Firewall Security

All personal computers are installed with virus protection and firewall software by the school's IT provider. Users are not to alter the configuration of this software. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If any user suspects viral infection on their machine, they should **disconnect their PC from the network and inform the school's IT provider immediately.** If your IT provider detects a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

Physical Security

Users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the school
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of external and removable drives which contain confidential school data
- Staff supervising pupils using ICT equipment should ensure pupils take reasonable care of such equipment

Remote Access

Remote access to the school network is possible where this has been granted by your IT provider.
Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.
All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.
Such records and information are sometimes required - under law - by external agencies and authorities. The school will comply with such requests when formally submitted.

Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence. Breaches of this policy will be dealt with in accordance with the Trust's disciplinary policy.

2. Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the Internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.
The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.
This Policy has been designed to safeguard the legal rights of members of staff.

Purposes

To provide guidance on inappropriate use of school telephones, email and internet facilities. To clarify when the school may monitor staff usage of these facilities.

Guidelines
Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.
The use of school telephones for private purposes, which are unreasonably excessive or for school purposes which are defamatory, obscene or otherwise inappropriate, may be treated as misconduct under the appropriate disciplinary procedure.
Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the school reserves the right to record calls.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.
Staff should be careful that before they open any attachment to a personal e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if a staff member receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the school. Any other use of e-mail for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.
Where the school has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.
The school also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of staff to undertake their school role. However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.
Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. The school reserves the right to audit the use of the Internet from particular Personal Computers or accounts where it suspects misuse of the facility.

Monitoring the use of telephone, e-mail and the Internet.

It is not the school's policy, as a matter of routine, to monitor an employee's use of the school's telephone or e-mail service or of the Internet via the school's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Head teacher may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Head teacher. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Head teacher.

3. Safe use of Management Information

Systems

4. Principles

This applies wherever access to the school Management Information Systems (MIS) are provided. This applies to all online resources provided by the school, for example Capita SIMS. This policy applies whenever information is accessed through the school MIS, whether the computer equipment used is owned by the school or not. The policy applies to all those who make use of the school's MIS resources.

Purposes Security

- This Policy is intended to minimise security risks. These risks might affect the integrity of the school's data, the authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from:

  - the intentional or unintentional disclosure of login credentials
  - the wrongful disclosure of private, sensitive, and confidential information
  - Exposure of the school to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

- This Policy aims to ensure all relevant aspects of the Data Protection Act (1998), GDPR and Fair Processing Policy are adhered to.
- This Policy aims to promote best use of the MIS system to further the communication and freedom of information between the school and Parents/Carers.

Guidelines

The school's online systems are provided for use only by persons who are legally responsible for pupil(s) currently attending the school.

Access is granted only on condition that the individual formally agrees to the terms of this Policy by signing at the end of this policy.

The authorising member of school staff **must** confirm that there is a legitimate entitlement to access information for pupils.

Personal Use

Information made available through the MIS system is confidential and protected by law. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the pupil to which the information relates **(ONLY if it is done so in a way intended to support learning or good pastoral care**) or to other adults with parental/carer responsibility.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk. Particular care should be exercised when using a projector or interactive whiteboard connected to a computer with the MIS open, for example if using the MIS to take the attendance register.

Password Policy

Staff must assume personal responsibility for usernames and passwords.
Never use anyone else's username or password.

You must always keep your individual user name and password confidential.
These usernames and passwords should ***never*** be disclosed to anyone.
Passwords and user names should never be shared.

In some instances users may be given the right to change passwords from the one originally issued.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to the school in writing to the Head Teacher.

The school reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

- the validity of parental/carer responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

<u>Electronic Information Security Declaration</u>

By signing the acceptance form you are agreeing that you have fully understood and accept the terms and conditions and all the instructions of the school Electronic Information Security Policy.
Please contact the Heed teacher if you are not sure of any policies and terms and conditions of use.

Signature……..
Name……..
Date…….

Annexe 2

Subject Access Requests

At a glance

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing.

In brief

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

You must verify the identity of the person making the request, using ‘reasonable means’.

If the request is made electronically, you should provide the information in a commonly used electronic format.

The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Further Reading

Relevant provisions in the GDPR - see Articles 12 and 15 and Recital 63
External link

We've created a form that you can make available for individuals to use if they wish to submit a subject access request, as per their rights under the General Data Protection Regulation.

You could make a paper copy available from the school office, or post a digital version on your school website. Ask individuals to hand their completed form in to the school office, which can then be passed directly to your data protection officer, or email it directly to the data protection officer.

Please note that you cannot insist that individuals use this form, and must still accept requests in other formats.

The form is based on guidance from the ICO, and their template form.

[Insert date]

Schools: insert your name and address

Re: subject access request

Dear *schools: insert the name of your data protection officer,*

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Name

Annexe 3
Data Protection Impact Assessment (DPIA) screening questions

Ref: Conducting privacy impact assessments code of practice
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

These questions are intended to help decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

1.	Will the project involve the collection of new information about individuals?
2.	Will the project compel individuals to provide information about themselves?
3.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4.	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5.	Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
6.	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
7.	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

8. Will the project require you to contact individuals in ways which they may find intrusive?

DPIA template

This template is for recording the DPIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA. The template follows the process which is used in the ICO *Conducting privacy impact assessments code of practice*.

Step one: Identify the need for a DPIA

- What does the project aim to achieve?
- What will be the benefits to the organisation, to individuals and to other parties?

You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

- Describe the collection and use of personal data (it may also be useful to refer to a flow diagram or another way of explaining data flows.
- How many individuals are likely to be affected by the project?
- Who will have access to the data?
- How will the data be processed?
- Where and by whom with the data be processed?
- With which third parties will the data be shared?
- For how long will the data be kept?
- Will data be anonymised?
- How will data be destroyed?

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks.

- Who should be consulted, internally and externally?
- How will you carry out the consultation?

You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the DPIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register. **Note**: Annex three of the ICO PIA code of practice can be used to help identify the GDPR related compliance risks.

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary
(e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the DPIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the DPIA outcomes back into the project plan
Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns:

Competed by (name and role):

Date:

Annexe 4

What are the lawful bases for processing data?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, read the relevant page of this guide

Annexe 5

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 Data Champion. The Data Champion will report the potential breach to the DPO immediately. The Data champion will investigate the report, and determine whether a breach has occurred. To decide, the DC 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 DC will alert the headteacher and the chair of governors as well as the DPO
- The DPO will work with the DC to 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's 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 (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the central Trust.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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 by the central Trust. The DPO and Data Champion/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*
- *If the sender is unavailable or cannot recall the email for any reason, the DC will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DC 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 DC will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DC 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 might include the following and will be investigated immediately by the DC and dealt with according to the nature of the breach, including removing/recalling information immediately.

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*