Worlingham CEVC Primary School

GDPR and Data Protection Policy

Approved by:	Schools' Choice	**Date:** 28.6.18
Last reviewed on:	10.11.20 Personnel Committee	
Next review due by:	1.12.20 Full Governing Body	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the body their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Schools' Choice and is contactable via:

Telephone Number: 01473 260700

Email: data.protection@schoolschoice.org

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our 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

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the 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**

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.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's retention guidance (taken from the Information Management Toolkit for Schools (IRMS) - see Appendix 1.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 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 the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

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

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

9.2 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.

9.3 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 one calendar month starting on the day 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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. 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 for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school 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.

See our Child Protection and Safeguarding and Photography and Digital Recording Policies for more information on our use of photographs and videos.

12. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils 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, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety policy, Computing policy and ICT 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 (see section 8)

14. Clear Desk Policy

The School is working towards a clear desk policy for all employees for the following reasons:

- it reduces the threat of a security breach as passwords and other confidential information are locked away or otherwise securely stored
- it ensures compliance with data protection requirements because personal data must be held securely at all times
- it protects employees' health and safety by reducing the risk of workplace accidents
- it reduces the risk of damage or destruction to information in the event of a disaster such as a fire or flood etc.
- it portrays a professional image to our parents, visitors and suppliers when they visit the School's premises

14.1 Procedure

At the end of your working day or where you leave your workplace for an extended period during the day, you must tidy your workplace and tidy away all school-related paperwork and files into your desk drawer, filing cabinet or cupboard in an efficient and organised manner. These should then be locked overnight where locking facilities are available. Confidential information or information containing personal data must always be securely stored. If you are unsure of the information's sensitivity, either ask your manager or lock it away securely.

Put any paperwork that you no longer need in your rubbish/recycling bin on a daily basis. Please use the School's shredding facilities or confidential waste bags where the information in the paperwork is confidential. Any unwanted paperwork that contains personal data or sensitive information should be shredded. Paperwork that you do need should be acted upon and then appropriately filed.

This policy includes removable storage media which may contain files downloaded from your computer, such as memory sticks, portable hard drives and CDs. Media of this type must also be cleared from your workplace before you go home.

Additionally, this policy is designed to reduce the amount of paper that the School uses, which in turn reduces the amount of printing costs and filing space needed. You should not print out hard copies of e-mails or documents just to read them unless this is really necessary. All information stored on the School's

computer and e-mail systems are backed-up so you will not lose the information unless you have specifically deleted it.

When printing out information, it should be cleared from printers immediately, particularly if the information is confidential or contains personal data. Faxes should also be taken from the fax machine immediately. Nothing should be left lying on printers, photocopiers or fax machines at the end of the day.

Finally, the floor space around/in your workplace should remain tidy and free from obstructions at all times.

It is your personal responsibility to adhere to this policy. If you fail to comply with the above rules, it will be dealt with in accordance with the School's disciplinary procedure.

15. Governor and School Staff Use of Email

The school provides e-mail and internet access to authorised users. The use of email within a school is an essential means of communication for staff, governors and students. In the context of school, emails should not be considered private and individuals should assume that anything they write or email could become public.

The purpose of this policy is to outline the procedure and protocols to be used when emailing and this policy must be adhered to by all authorised users.

15.1 Email Accounts

The school gives all staff and governors their own email account as a work-based tool.

This school email account should be the account that is used for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal contact information being revealed.

For the safety and security of users and recipients, all mail is filtered and logged. If necessary, email histories can be traced.

The following rules will apply:

- Under no circumstances should staff or governors contact students, parents or conduct any school business using any personal email addresses.
- It is the responsibility of each account holder to keep their password/s secure.
- All external emails, including those to parents, should be constructed in the same way as a formal letter written on school headed paper.
- If any issues/complaints are involved then staff sending emails to parents, external organisations, or students are advised to cc their line manager/s and other relevant individuals.
- The school requires a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the school. Please note that this disclaimer is automatically added to emails sent externally.
- All emails should be written and checked carefully before sending.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act or a Subject Access Request in certain circumstances.

Staff are expected to manage their staff email account in an effective way as follows:

- Delete all emails of short-term value.
- Organise email into folders and carry out frequent house-keeping on all folders and archives.
- Respond to emails in a timely fashion.
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school ICT, e-safety and email policies apply.

Staff must immediately inform their line manager if they receive an offensive email and any suspicious emails should be reported to the network manager and should not be opened.

15.2 Sending Emails

The following rules apply:

- When composing your message to a parent or non-staff member you should always use formal language, as if you were writing a letter on headed paper.

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please see the section below 'Emailing personal, sensitive, confidential or classified information'.
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send whole school emails unless essential for school business.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

15.3 Receiving Emails

The following rules apply:

- Check your email regularly.
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source. If unsure, always consult the network manager first.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The setting to automatically forward and/or delete of emails is not allowed.

15.4 Emailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data without the use of encryption is strictly prohibited.

Where the conclusion is that your school email must be used to transmit such data, then exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information.
- Verify (preferably by phoning) the details of a requestor, if unknown, before responding to email requests for information.
- Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify.
- Send the information as an encrypted/password protected document attached to an email. If you are unsure as to how to complete this, please speak to the network manager/ICT technician.
- Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone.
- Do not identify such information in the subject line of any email.
- Request confirmation of safe receipt.
- When sending an email containing personal or sensitive data, the name of the individual is not to be included in the subject line and the document containing the information must be encrypted.
- To provide additional security you need to put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. See Appendix 1 Management of the School Data retention periods for further information.

17. 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 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing body.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection and Safeguarding
- ICT and Online Safety Policy
- Clear Desk Guidance
- Records Management Policy
- Published Guide to Information

V3-OCTOBER 2020

Appendix 1 : School Retention Guidance

Please see separate document

Appendix 2: 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'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 on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take relevant actions (an example is 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.

For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases 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
- 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

Appendix 3: Data Classification

Classification	Description of Information Types
Green	No Impact - information formally made public by school or information which would have no impact on privacy or school reputation if it was to be put into the public domain by any other means.
Amber	Strictly internal or agreed partners - school information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - this could also include names, addresses and pupil numbers that pose little or no risk to privacy.
Red/Offical-Sensitive	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender or sexuality.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families.
	Employee & partner personal data - personal data on employees of the school and its partners. This includes details about ethnicity, gender or sexuality.
	Safeguarding information
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality.
	School information which would have a significant impact on the reputation or business of the school if it was seen by non-intended recipient because of commercial, legal, fraud, investigatory or other areas where confidentiality is necessary.

Appendix 4: Incident Grading Document

Incident grading 1 = Negligible
Any type of incident formally recorded, or something worthy of investigation but turns out to be a “false positive”, “near miss” or loss of equipment where there is a remote chance of the data being readable, which has negligible impact on privacy or school. **Reporting of such incidents is still valuable and should be used as part of ongoing information security risk assessment.*

Incident grading 2 = Minor	
Confidentiality	Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no health or safety impacts (e.g. just name, address, pupil number at amber level)
Integrity	Confirmed or likely issues relating to integrity of information on <10 staff or pupils such as confused identities, out of date information or records misplaced which causes localised inconvenience or delays.
Availability	Some localised and short-lived loss of availability, such as through a temporary systems failure, which leads to the disruption of non-critical teams/areas.

Incident grading 3 = Moderate	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals OR any breach of “OFFICIAL- SENSITIVE” information at red level. Likely local media interest and adverse publicity.
Integrity	Issues relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other implications.
Availability	Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of local team business continuity plans. This may be either a short disruption to a very critical team/area or a longer disruption to a group of less critical teams/areas.

Incident grading 4 = Major	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals OR loss of any sensitive personal data at red level which is highly likely to affect the health or safety of one or more individuals OR any privacy breach which because of the high profile nature of the person(s) affected or other circumstances is likely to lead to national media attention and cause significant reputational damage.
Integrity	An integrity issue which means data relating to 100+ staff or pupils is in effect no longer usable or understandable (and cannot be rectified) and is likely to impact health, and safety or key teams/areas/the school.
Availability	Sustained loss of availability of information which has serious impact on the delivery of a number of critical areas, resulting in business continuity plans being invoked for at least one business area.

Incident grading 5 = Extreme	
Confidentiality	Loss of data or privacy breach relating at large scale (i.e. 100,000+ persons or complete datasets); likely national/international media adverse publicity, prolonged damage (for example parent trust) and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.
Integrity	Integrity problem which leads to significant amounts of data on 100,000+ persons being unreadable or unusable and does directly lead to health and safety issues or significant services issues (e.g. entire data set for pupil group corrupted beyond use that must be re-created).
Availability	Outage or other issue which leads to general failure of IT so that teams/areas which are critical to the school are not running for a prolonged period. Business Continuity Plans across school/trust are invoked.

APPENDIX 5

Data Breach Incident Form

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against loss, destruction of or damage to personal data. A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

As soon as you are aware of a data breach you must notify your Lisa Hughes, Bursar with immediate effect.

Once you have notified the Lisa Hughes, Bursar this form should be completed and returned to data.protection@schoolschoice.org

Information Management Leads

Lead	Contact Information
Lisa Hughes, Bursar	Telephone: 01502 712375 lhughes@wcevcps.org
Schools' Choice	Telephone: 01473 260700 Data.protection@schoolschoice.org

1.	Name of the person who identified the breach	
2.	Job title and contact details	
3.	Establishment Name	
4.	When did the breach happen? Date: Time:	
5.	When did you discover the breach? Date: Time:	
6.	If there has been a delay in reporting this breach, please explain why	
7.	How did you find out about the breach?	
8.	Tell us as much as you can about what happened, what went wrong and how it happened.	
9.	Is this a breach of data by a supplier or partner organisation? (If the breach has been notified to you by a supplier or a partner organisation who you share your data with, name of the supplier/partner, date notified, contact should be completed)	The breach originated in your establishment: **Yes/No** We have been notified of the breach by a supplier / Partner Organisation. **Name:** **Name Contact:** **Date Notified:** **[Insert Link to the saved notification]**
10.	Was the breach caused by a cyber incident e.g phishing	**If yes please also complete section "Cyber incidents only"**
11.	Who has been notified of the breach to date? (e.g. Headteacher, DPO, ICO, Parents, Teachers, Governors etc.)	

	Have you told, or are you planning to tell any other organisations about the breach? eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies	
12.	Have you made data subjects aware of the breach?	
13.	Number of personal data records concerned?	
14.	How many data subjects could be affected?	
15.	Categories of personal data Please highlight those that are relevant.	Data revealing racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Sex life data Sexual orientation data Gender reassignment data Health data Basic personal identifiers, eg name, contact details Identification data, eg usernames, passwords Economic and financial data, eg credit card numbers, bank details Official documents, eg driving licences Location data Genetic or biometric data Criminal convictions, offences Not yet known Other (please give details below)

16.	Categories of data subjects	Employees Students Parents or prospective parents Children Vulnerable adults Not yet known Other (please give details below)
17.	If the data has been lost or stolen, were there any protections in place such as encryption?	
18.	Describe the actions you have taken, or propose to take, as a result of the breach *Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.*	
19	Summarise the lessons learnt	
20.	What is the likelihood that data subjects will experience significant consequences as a result of the breach? Please highlight i.e Risk to physical safety as a result of the breach Risk of the data being used to discriminate against an individual Risk to the reputation of any individual being impacted by the breach Risk of financial loss through identity theft	**The ICO will need to be notified within 72 hours of all data breaches where a risk to individual's rights and freedom exists.** Very likely Likely Neutral (neither likely nor unlikely) Unlikely Very unlikely Not yet known Please describe any possible impact on data subjects:

21.	Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	
22	Had the staff member involved in this breach received data protection training in the last two years?	
23.	Further comments:	

Cyber Incidents only:

1.	Has the confidentiality, integrity and/or availability of your information systems been affected?	Yes No Don't know If you answered yes, please specify: Confidentiality Integrity Availability
2.	Impact on your organisation Please highlight	**High** – You have lost the ability to provide all critical services to all users **Medium** – You have lost the ability to provide a critical service to some users **Low** – There is no loss of efficiency, or a low loss efficiency, and you can still provide all critical services to all users **Not yet known**

3.	Recovery time	Regular – you can predict your recovery time with existing resources Supplemented – you can predict your recovery time with additional resources Extended – you cannot predict your recovery time and need extra resources Not recoverable – recovery from the incident is not possible eg. back ups cannot be restored Complete – recovery is complete Not yet known

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

To be completed by the DPO
Date received and logged: Does this represent a 'High Risk' to the rights and freedoms of those impacted individuals? If yes details of the communication plan: Future mitigating actions identified: What Type of Data Breach is it?

A **Confidentiality Breach** has occurred if the data was unauthorised of accidentally disclosed.

An **Availability Breach** has occurred if the data was unauthorised or accidentally lost.

An **Integrity Breach** has occurred if the data was unauthorised or accidentally altered.

Date ICO notified:

Further comments:

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

Review Date: _____

Appendix 6: Subject Access Request Form

Name:
Telephone Number:
Email:
Address:
Employee Payroll Number *(If relevant)*:
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the school that you are eligible to receive.
Required information (and any relevant dates): *Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.*
By signing below, you indicate that you are the individual named above. The school cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnity us for all losses, cost and expenses if you are not. Please return this form to data.protection@schoolschoice.org Please allow 1 calendar month for a reply.
Data Subject's Signature:
Date:

Appendix 7: Checklist for Subject Access Requests

Step/Area to Consider	Complete (if relevant) Y/N	Notes
How was the request received? (e.g. using a template form, by email, over the phone etc.)		
Is the request a subject access request for some/all personal data (and/or information about how it is used) or a routine enquiry to the school (for which a different procedure may apply)?		
Is the scope of the request clear, or is any additional information required to locate the information requested and to deal with the request? *If there is any doubt as to the status of the request or the scope of this, you may need to clarify the position with the individual.*		
Has a record been made of the date on which a request was made and when the response is due?		
Has the identity of the requester been verified?		
Has receipt been acknowledged?		
Does the school hold personal data about the requester? If not, has the requester been informed?		
Where is the personal data held? i.e. electronic records, paper filing systems, emails etc.		
Have all relevant manager's/team leaders been communicated to that they will need to help find this data?		
Have all appropriate locations been searched? What search terms were used? i.e. to locate emails in an inbox.		
Is any of the information which is the subject of the request due to be changed or deleted between the date of the request and the provision of the information? Have you sought to retrieve such information prior to deletion (where possible) and without undue delay?		
Is any third party personal data included within the request? If so, has this been assessed in regard to whether such information may be disclosed? *In this instance you should take into account any express refusal of consent to disclose this information or any duty of confidentiality owed to the third party in question.*		
Have all relevant exemptions been considered? *If applicable*		

Have the reasons for the application of exemptions been documented, including the basis for any refusal to release third party data? Have exemptions been applied consistently?		
Does the application of exemptions involve the redaction or extraction of any information? If so, has this been applied appropriately?		
Does the information being disclosed include any codes, acronyms or complex language which may require explanation? Have steps been taken to ensure that the information that is being disclosed is concise and clear?		
In what format will the requested information be provided? If the request was received electronically, is this being provided electronically? Is the information sufficiently secure in transmission?		
Does the covering letter include information about the processing? (such as purposes, disclosures, source etc.)		
Has the response been reviewed internally in accordance with applicable procedures before being sent to the individual?		
Has the register of subject access record been updated?		

Appendix 8: Data Sharing Decision Form

Name of requesting organisation:	
Name and position of person requesting data:	
Data requested:	
Purpose:	
Decision:	
Data supplied:	
Decision taken by *(name and position)*:	
Date of disclosure:	
Any specific arrangements: *(re. retention/deletion of data)*	
Reason(s) for disclosure or non-disclosure:	
Date request responded to:	
Signed:	
Dated:	