Brampton Abbotts CE Primary School

Bridstow CE Primary School

Oak Meadow Federation

DATA MANAGEMENT POLICY SUITE

This policy will be reviewed and updated by the governing body at least annually.
All references to 'the school' imply both Brampton Abbotts and Bridstow Primary Schools.

Date signed off by full governing body: 17th October 2023

Signed Daniel Brearey, Head teacher

Paul Mason, Chair of governors

Date next review due: October 2024

Introduction

Our vision is rooted in Psalm 1:3: 'You are like a tree, planted by streams of water that never run dry. Your fruit ripens in its time; your leaves never fade or curl. In all you do, you prosper'. To this end, and in order to create a positive learning environment, this policy suite sets out the school's approach to ensuring that all data are handled respectfully and sensitively, so that pupils, staff and volunteers flourish.

This suite of policies aims:

- to ensure that all staff and volunteers understand their responsibilities in relation to data protection;
- to ensure the school has appropriate training, documents, procedures and IT systems in place to support safe management of data;
- to safeguard both children and adults by ensuring that their data are managed responsibly;
- to safeguard the school against hacking, cyber-attack or accidental destruction of data management systems;
- to ensure that, where appropriate, data are shared in a safe, open and fair manner.

This policy suite contains the following chapters.

Complaints and whistleblowing

Complaints should follow the procedures as set out in the Complaints Policy on our website. Staff also have a responsibility to raise any concerns following the school's whistleblowing policy. Complaints relating to information handling may be referred to the ICO (the statutory regulator).

Compliance

This policy suite complies with the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR"), the Data Protection Act 2018 ("the DPA") and other related legislation which protects Personal Information. It also meets DfE requirements for identifying which documents will be published on the website, and Freedom of Information Act requirements.

The school takes compliance with this policy suite very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

Anyone with questions or concerns about this policy should contact the school's Data Protection Officer, HY Education, by email at DPO@wearehy.com, by telephone on 0161 543 8884 or in writing at HY Education, 3 Reed House, Hunters Lane, Rochdale OL16 1YL.

This suite of policies applies to all staff, volunteers and contractors who have any access to school data. For brevity, the policy refers to 'staff' but includes all groups listed here.

CHAPTER 1: DATA MANAGEMENT PRINCIPLES AND APPROACH

1.1 A whole school approach: safeguarding and supporting pupils

It is vital to our mission and purpose as a school that we keep children safe and enable them to achieve their potential. To do this, the school holds personal information to understand each child's needs, as well as information on staff, parents and others who come into contact with the school.

As part of keeping everyone safe, it is vital that these data are handled sensitively and securely. This means that everyone in school has to take responsibility for this.

1.2 Principles: confidentiality, integrity and accountability

Staff must maintain data security by protecting the confidentiality, integrity and availability of personal information. The guiding principles of the information security can be summarised as:

- confidentiality, which means that only people who have a need to know and are authorised to use personal data can access them;
- integrity, which means that personal data are accurate and appropriate for the purpose for which they are processed, are lawful, safe, fair and transparent, and are only held and kept for as long as necessary (i.e. are minimal, and limited in purpose and storage);
- accountability, accuracy and compliance, which means that the school holds accurate data, complies with relevant legislation, and demonstrates this compliance.

1.3 Personal information

Data protection legislation covers personal information. Personal information is defined as information which relates to a living individual who could be identified from the data or other information held. In order to hold and process personal information, the school has to identify a legal basis for doing so. For schools, this is most likely to be because it is necessary to exercise a legal obligation, public task, performance of a contract, to protect vital interests or because specific consent has been given.

The school collects a large amount of personal data every year, including pupil records, staff records, fee collection, and the names and addresses of those requesting prospectuses, examination marks or references. In addition, it is required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

The school will only collect and process Personal Information for specified, explicit and legitimate reasons and will not further process Personal Information unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

Some categories of personal information are considered to be particularly sensitive. These data include information about race, ethnic origin, political persuasion, religious belief, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation. The Data Protection legislation deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.

Where it is necessary to obtain consent to process Personal Information, the school will ensure that it is always done in accordance with data protection laws.

1.4 Photographic & digital information

The school uses photographs and videos of children for marketing and social media, and only with the express consent of parents / carers, per the form at Appendix 3. These are considered

data per legislation but in terms of this policy are separate from other data collected by the school, as they are only used for the specific purpose of showcasing the pupils and the school and are not held for more than 12 months after a child has left the school. Historic photographs may, however, remain on our website, on social media feeds or, in some cases, when forming part of decorative displays.

1.5 Biometric information

The school does not currently collect any biometric information. However, this will be kept under review, and appropriate procedures will be developed should this change.

1.6 Privacy Notices

The school will use privacy notices to inform data subjects about data collection and use. The school's privacy notices can be found on the school's website.

In many cases, the school will hold and process information because it is necessary for it to carry out a legal obligation, a public task, for reasons related to contract or to protect an individual's vital interests. This does not remove the need to explain to people (whether staff, contractors, volunteers, parents / carers or pupils) how their data are being used, why, and for how long they will be stored. This information is included in the school's privacy notices.

In some specific cases, explicit consent is the legal basis for processing personal data. Where this is the case, a specific consent form that specifies what data are needed and why, and how they will be stored and for how long, should be signed by the relevant individuals.

Should the school wish to use these data for any purpose other than that specified when it was originally obtained, the data subject's explicit consent should be obtained prior to using the data in the new way. Should the school wish to share personal data with anyone other than those recipients specified at the time the data were originally obtained, and where there is not a non-consent-based justification for sharing the data, the data subject's explicit consent should be obtained prior to sharing those data. Failure to do so could result in a breach of confidentiality.

1.7 Accuracy and data quality

Where practical and feasible, the school will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the data subject. If anyone whose data are held exercises their right for their data to be erased, rectified, or restricted, or if someone objects to the processing of their data, the Data Protection Officer must be notified and the appropriate procedures must be followed. All updates to information received, by anyone, should be added to the correct system and passed to the correct member of staff for updating and processing within 10 working days (term time only).

1.8 Data storage and retention

The school sets out requirements for safe data storage, both electronic and manual filing. This includes restrictions on who can access the information physically and electronically.

The school also maintains a Retention Schedule to ensure that personal data are securely deleted or destroyed at required times. Staff members take all reasonable steps to destroy or delete all personal data that are held by the school (whether physically or electronically) when they are no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable. The Schedule does not include photographs of children, which are not stored for more than 12 months after a child has left the school. Historic photographs may however remain on our website, on social media feeds or, in some cases, when forming part of a decorative displays.

1.9 Information sharing

It is critical that all personal information is kept confidential and secure, and only shared when there is a good reason to do so. The following principles are followed when determining whether to share information.

- The school is open and honest with the person whose data are being shared (or their parents / carers, where appropriate) about why, what, how and with whom information will or could be shared.
- Staff members must seek advice from the Data Protection Officer if they are in any doubt as to whether to share information, without disclosing the individual's identity if possible.
- As set out in the Child Protection policy, personal information can be disclosed without consent if there is a risk of immediate harm. However, staff members should always be mindful that the individual concerned may not have expected their information to be shared. Staff members should never promise a child that they will not tell anyone about a report of abuse, as this may not be in the child's best interests.
- All staff members must ensure that the information shared is necessary for the purpose for which they are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
- A record of the decision and the reasons for it will be kept, whether that decision is to share information or not. If staff members decide to share information, they will record what has been shared, with whom and for what purpose.
- Where it is decided to share information, this should be done securely and following an appropriate transfer process.

In addition, data should not be transferred to other countries unless they have appropriate data protection safeguards in place. The Data Protection Officer will be able to advise if there is a need to transfer information outside the UK.

1.10 Individuals' rights

Everyone whose information is held by the school has the right in relation to their personal information, and school will follow appropriate procedures to ensure these rights are observed:

- to be informed about how, why and on what basis that information is processed *(link to privacy notices);*
- to obtain confirmation that personal information is being processed and to obtain access to it, by making a subject access request;
- to have data corrected if they are inaccurate or incomplete;
- to have data erased if they are no longer necessary for the purpose for which they were originally collected/processed, or if there are no overriding legitimate grounds for the data to be retained ('the right to be forgotten');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased) or where the school no longer needs the personal information, but the data are required to establish, exercise or defend a legal claim;
- to restrict the processing of personal information temporarily where they do not think it is accurate (and the school is verifying whether it is accurate), or where they have objected to the processing (and the school is considering whether its legitimate grounds override their interests);

- in limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used format;
- to withdraw consent to processing at any time (if applicable);
- to request a copy of an agreement under which personal data are transferred outside the country;
- to object to decisions based solely on automated processing, including profiling;
- to be notified of a data breach which is likely to result in high risk to their rights and obligations;
- to make a complaint to the Information Commissioner's Office (ICO) or a court.

Children have the same rights as adults over their personal data. In circumstances where a person with parental responsibility exercises rights on behalf of a child, it may be considered appropriate to seek the child's consent before complying with a request.

1.11 Data breaches

A personal data breach occurs when there has been breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Such breaches can be both accidental or deliberate and may take many different forms, for example:

- loss or theft of data or of equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or a third party;
- loss of data resulting from an equipment or systems failure (including hardware or software);
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams;
- blagging offences where information is obtained by deceiving the organisation which holds it.

The school takes data security seriously and ensures that all incidents however minor or major are reported to the nominated individual as soon as they are discovered. The school must report a data breach to the ICO without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. This should include the factual background to the breach, who has been affected by the breach, the number of people affected, the type and sensitivity of the data, the potential or actual consequences, and the measures put in place to minimise the breach. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms and should notify the governing body of any data breach.

Staff members should ensure that they inform the Data Protection Officer immediately if a data breach is discovered and make all reasonable efforts to recover the information. A standard form for reporting data breaches is available on the ICO website here.

1.12 Data protection by design and information and records management

The school has procedures in place that requires data protection to be built into our systems and processes up-front, including requiring staff to complete Data Protection Impact Assessments. Further details on how we embed data protection throughout our work can be found in the appendices. Our retention schedule ensures that all data are recorded and stored appropriately.

CHAPTER 2: FREEDOM OF INFORMATION: RESPONDING TO REQUESTS FOR INFORMATION

2.1 Information covered by the Freedom of Information Act

The Freedom of Information Act requires public authorities (including schools) proactively to publish certain information and provide a publication scheme. It also gives the public a right of access (subject to some exemptions) to copies of recorded information held by the school or held on its behalf by another person or organisation. It covers all recorded information both written and digital, including emails (and drafts of emails), notes, recordings of 'phone conversations (or Zoom/Teams calls), letters sent and received, online messages and social media. For documents that have been created electronically, it also covers information (known as meta data) that can be recovered from the document's properties (e.g. who created the document and when).

2.2 Responding to requests under the Freedom of Information Act

A full procedure for responding to Freedom of Information requests can be obtained from the school office. In summary, the school aims to respond to all requests for information within 20 school days (excluding school holidays) or 60 working days if this is shorter, even if it is to say that you do not have the information. All requests must be in writing (including email) and must have an address for a response to be sent to. However, they do not need to mention the Freedom of Information Act.

No new information has to be created in order to respond to a request. However, unless it is covered by a specific exemption (see 2.3 below), any information requested that already exists must be released.

If information will take more than 18 hours to collate, you can refuse the request or request payment (see below).

2.3 Refusing requests under the Freedom of Information Act

Under limited circumstances, we may refuse a request for information if:

- the request is vexatious;
- the request is a repeat request from the same person;
- it would cost more than £450 to comply (this includes staff time, which must be costed at £25 an hour or 18 hours, regardless of the pay of the member of staff who would undertake the work);
- the information requested is covered by an exemption, e.g. because of commercial or personal sensitivity or an ongoing criminal investigation, balanced against the public interest.

CHAPTER 3: FREEDOM OF INFORMATION: SCHEME OF PUBLICATION

3.1 Proactively publishing information

In addition to responding to requests for information, the school proactively publishes information, using the template provided by the Information Commissioner's Office.

3.2 Charging for information

All of the information in our Publication Scheme is available free of charge from our website. If you need a printed copy, there is no charge for a single copy. However, multiple copies will be charged at the current rate for photocopying. There will also be a charge for any information that we would normally sell, e.g. videos. A full schedule of charges can be obtained from the school office.

Appendix 1: Legislation and statutory guidance

This policy is based on the statutory guidance:

Data Protection Act (2018)

Information Commissioner's Office

Keeping Children Safe in Education (2023).

Supplementary Guidance

In addition to the school's published Data Protection suite, the school also adheres to the following policies produced by HY Education, our Data Protection Officer:

CCTV Policy

Consent & Biometric Data

Data Breach Procedure

Data Protection Policy

Information Security Policy

Privacy Notices

Retention Schedule

Subject Access Procedures

Appendix 2: DEFINITION OF DATA PROTECTION TERMS

Data Subjects means an identified or identifiable natural person. For example, we process personal information about parents, staff members and pupils each of whom is a data subject.

Personal Information means any information about a data subject. Examples of personal information could include information about a pupil's attendance, medical conditions, Special Educational Needs requirements or photographs.

Privacy Notices are documents provided to data subjects which explain, in simple language, what information we collect about them, why we collect it and why it is lawful to do so. They also provide other important information which we are required to provide under data protection laws. Our privacy policies are available on our website and from the School upon request.

Data Controllers determine the purpose and means of processing personal information. They are responsible for establishing practices and policies in line with the GDPR. The School is a Data Controller.

Data Users are those of our staff members whose work involves processing personal information. Data users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

Processing means when personal information is used in a particular way. For example, we may need to collect, record, organise, structure, store, adapt or delete personal information. When we do this, we will be Processing.

Special Category of Personal Information means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a data subject's sex life or sexual orientation. These types of personal information are regarded as being more 'sensitive' and the law requires increased safeguards to be in place if we are to process this type of data.

Data protection impact assessments are carried out when engaged in high risk processing.

DPIAs will include: a description of the nature of the processing, its scope, context and purposes; an assessment of the necessity and proportionality of the processing in relation to its purpose; an assessment of any data processors we use as part of the processing; an assessment of the risk to individuals; and the risk mitigation measures in place and demonstration of compliance.

Appendix 3: Consent form for photographs and videos

During your child's time at school, we may wish to take photographs or record videos of activities that involve your child. The photographs or videos may be used for displays, promotional material, our website, social media and in the newspaper.

Photography or filming will only take place with the permission of the headteacher and under appropriate supervision. When filming or photography is carried out by the media, children will only be named if there is a particular reason to do so (e.g. if they have won a prize), and home addresses will never be disclosed. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before taking any photographs of your child for these purposes, we need your consent. This is necessary to comply with data protection laws (i.e. the UK General Data Protection Regulation and Data Protection Act 2018). Without your consent, we will not be able to use your child's photograph for these purposes.

Please note that there may be other circumstances, falling outside the normal day-to-day activities of the school, in which pictures of children are requested. No photograph of a child will ever be shared without parental consent.

We would be grateful if you confirm your preferences by ticking the appropriate boxes below:-

I consent to the use of my child's photograph for…	Yes	No
The school's social media		
The school's website		
The school's promotional material / prospectus		
School displays (which may include your child's work and first name)		
Other pupils' learning portfolios which get sent home to parents		
Publication in the school newsletter		
Publication in a newspaper (including any outline versions)		

If you give consent for photographs to be used as described above, you may withdraw your consent at any time. If you decide to withdraw your consent, please contact the school office so that we can update our records accordingly.

When you provide your consent, this will remain valid for the duration of your child's attendance at the school and for 12 months after your child leaves the school (unless you choose to withdraw your consent earlier). Historic photographs may, however, remain on our website, on social media feeds or, in some cases, when forming part of decorative displays.

Appendix 4: Roles and responsibilities

Role	**Responsibilities** (not exhaustive list but key ones for our school)
Data protection officer	Inform and advise the school, staff, governors, volunteers and contractors of their data protection responsibilities Provide advice and monitor the need for the carrying out of data protection impact assessments Act as the contact point for the Information Commissioner's Office Monitor compliance with school policies and procedures in relation to the protection of personal data, ensuring that responsibilities are assigned and raising awareness of the data protection elements of policies Train staff involved in processing information Conduct data audits Provide advice and assistance with data subject rights requests
Senior Leadership	Ensure that staff are adequately trained regarding their data protection responsibilities Provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice Ensure that appropriate IT and manual filing systems are in place and kept up-to-date to protect data, and to enable secure transfer of data Ensure that appropriate audits and monitoring activities are undertaken to be sure that data are being collected, stored and processed appropriately
Governing Body	Provide support and challenge to senior management and Data Protection Officer in the exercise of their functions.
All staff, governors and volunteers, agency staff, and those working on behalf of school	Only access and process data as their role requires Only allow other staff to access personal information if they have appropriate authorisation Only allow individuals who are not school staff to access personal information if they have specific authority to do so Keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies) Do not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device

	Do not store personal information on local drives or on personal devices that are used for work purposes Ensure personal information is recorded accurately and is kept up to date Refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer Raise actual or potential breach of the Data Protection Act to the Data Protection Officer as soon as the breach is discovered
Contractors	Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. Contracts with external organisations must provide that: • the organisation may only act on the written instructions of the school; • those processing data are subject to the duty of confidence; • appropriate measures are taken to ensure the security of processing; • sub-contractors are only engaged with the prior consent of the school and under a written contract; • the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection; • the organisation will delete or return all personal information to the school as requested at the end of the contract; • the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that it is both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law; • before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the Data Protection Officer.

Appendix 5: Practical steps

Requirement/ good practice	**Who is responsible**	**What the school does**
Audit and maintain a record of all personal data held	SLT / Governors	The record of personal data held is updated annually, showing the information held, who accesses it, where it is held, why it is held and for how long, and any appropriate safeguards to protect the information. This also records the lawful basis under which the data are processed, including the specific requirements for sensitive data.
Put in place procedures where personal information is held to ensure it is stored, accessed and processed securely	SLT / Governors	Procedures are reviewed whenever a process changes, or annually when this policy is reviewed.
Undertake Data Protection Impact Assessments (DPIAs) as needed	Staff member setting up new process, supported by Data Protection Officer	A risk assessment is completed when the school's processing of personal data could involve risks to rights and freedoms of individuals, such as when third party processors and new technologies are used.
Make Privacy Notices readily available	SLT / Governors	
Store and collect consent and withdrawal of consent		
Maintain a Data Retention Schedule	SLT / Governors	Schedule is updated as needed and reviewed annually, including ensuring that it includes appropriate procedures for destroying information no longer required.
Check data quality	All staff	
Only share information when appropriate to do so	All staff	All staff are made aware of the principles set out in this policy and must consult the Data Protection Officer for advice. Records are kept of any information shared. Procedures for secure transfer of information are reviewed annually.
Put in place procedures to comply with the duty to respond to data subject rights requests	SLT / Governors	Implement procedures, ensure all staff are trained in the procedures and review the procedures on an annual basis to ensure their suitability and compliance with legislation
Provide training	SLT / Governors	Staff, volunteers and governors are given appropriate training, as needed, to effectively fulfil their responsibilities in this policy.

Appendix 6: Key contacts

ROLE/ORGANISATION	NAME	CONTACT DETAILS
School Data Protection Officer		DPO@wearehy.com 0161 543 8884
Local authority data protection team	n/a	informationgovernance@herefordshire.gov.uk
Information Commissioner's Office	n/a	0303 123 1113

Appendix 6: ICO data breach reporting template

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. ***Please do not include any of the personal data involved in the breach when completing this form****. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.*

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

Initial report – report complete

Follow-up report – report complete

Initial report – additional information to follow

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

I consider that the incident meets the threshold to report

I do not consider the incident meets the threshold to report, however I want you to be aware

I am unclear whether the incident meets the threshold to report

Size of organisation

Fewer than 250 staff

Is this the first time you have contacted us about a breach since the GDPR came into force?

Yes

No

Unknown

About the breach

Please describe what happened

Please describe how the incident occurred

How did the organisation discover the breach?

What preventative measures did you have in place?

Was the breach caused by a cyber incident?

Yes

No

Don't know

When did the breach happen?

Date: Time:

When did you discover the breach?

Date: Time:

Categories of personal data included in the breach (tick all that apply)

☐ 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, eg coordinates
☐ Genetic or biometric data
☐ Criminal convictions, offences
☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

Number of personal data records concerned

How many data subjects could be affected?

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected

Categories of data subjects affected (tick all that apply)

☐ Employees
☐ Users
☐ Subscribers
☐ Students
☐ Customers or prospective customers
☐ Patients
☐ Children
☐ Vulnerable adults
☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

Is the personal data breach likely to result in a high risk to data subjects?

Yes

No

Not yet known

Please give details

(Cyber incidents only) Recovery time

We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident

We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this

We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, i.e. backups failed, no current backup, backup encrypted etc.

We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

Yes

No

Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Describe any further action you have taken, or propose to take, as a result of the breach

Have you told data subjects about the breach?

Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects

Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway

No – but we are planning to because we have determined it is likely there is a high risk to data subjects

No – we determined that the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

Yes

No

Don't know

If you answered yes, please specify

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

Yes

No

If yes:

Please confirm the Code / Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

Yes

No

Have you informed the relevant Monitoring Body or Certification Body?

Yes

No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

Report a suspicious website - NCSC.GOV.UK

About you

Organisation (data controller) name

Registration number

If not registered, please give exemption reason

Business sector

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow-up report

If this is a follow-up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case.)

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days sto provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.