BUSHFIELD ROAD INFANT SCHOOL

General Data Protection Regulation and Record Management

AUTUMN 2019

General Data Protection Policy (GDPR)

Aims

As the Data Controller, Bushfield Road Infant School is required to keep and process certain information about staff members and pupils in accordance with legal obligations under the General Data Protection Regulation. We are committed to the protection of all personal and sensitive data for which we holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

This policy is in place to ensure all staff and governors are aware of their responsibilities in relation to the core principles of the GDPR. Failure to do so may lead to disciplinary action.

This policy complies with the requirements set out in the GDPR, which came into effect on 25th May 2018. Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address.

The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) the legal bases for processing data are as follows:

a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose:

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre- ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was

given.

- Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time. The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

b) The right to removal of personal data

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing or storage.

Individuals have the right to erasure in the following circumstances:-

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Where the personal data was unlawfully processed
- Where the personal data is required to be erased in order to comply with a legal obligation.

Contract: the processing is necessary for the member of staff's employment contract or pupil placement contract.

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

1. **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 - UPN number - Location data - Online identifier, such as username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories 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 - Biometrics (such as fingerprints, retina or iris patterns), where used for identification purposes. - 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.

2. **Principles**

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- The GDPR also requires that 'the controller shall be responsible for, and able to demonstrate, compliance with the principles'.

3. Data protection officer (DPO)

All staff have the responsibility to treat all pupil information in a confidential manner and follow the guidance as outlined within this policy. The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided through online resources.

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

The DPO is the first point of contact for individuals whose data the school processes, and for the ICO (Information Commissioner's Office).

The DPO is responsible for monitoring this policy:

- Mr T C Pinto

The Head teacher of the school is responsible as the Data Controller on a day-to-day basis:

- Mrs T Bass (Head teacher)

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

4. **Whole staff responsibilities:**

All staff are responsible for:

- Collecting, storing and processing any personal information in accordance with this policy

- Informing the school of any changes to their personal data, such as a change of address

- Informing the Head teacher (Data Controller) with regards to:
    - Any questions about the operation of this policy, data protection law, retraining personal data or keeping personal data secure
    - Any concerns about breaches of the policy
    - Being unsure whether or not they have a lawful basis to use data in a particular way
    - Reporting a data breach
    - Engaging in a new activity which may affect the privacy rights of an individual
    - Help with any contracts or sharing personal data with third parties

5. **Notification:**

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about- the-ico/what-we-do/register-of-data-controllers/
Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

6. **Personal and Sensitive Data:**

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

7. **Fair Processing / Privacy Notice:**

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency- and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Personal data must not be shared with anyone else and can only be considered if:

- There is an issue with a pupil or parent/carer that puts the safety of staff at risk
- There is a need to liaise with other agencies (consent may be required prior to doing this)
- Suppliers or contractors need data to enable services to be provided to staff and pupils: for example, IT companies.

The school will:

- Only appoint suppliers or contractors which can provide sufficient guarantees of compliance with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone agreement, to ensure the fair and lawful processing of any personal data shared
- Only share data that the supplier or contractor needs to carry out their service.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information, including:

- The prevention of a crime or detection of a crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- Information connection with legal proceedings
- Disclosing information required to satisfy safeguarding obligations
- Research and statistical purpose, as long as the data is anonymised or consent has been provided
- Emergency services and local authorities to help them respond to an emergency situation that affects any pupil or staff member.

If personal data is transferred to a country or territory outside the European Economic Area, it must be done so in accordance with data protection law.

Any proposed change to the processing of individual's data shall first be notified to them.

Information may not be disclosed if:

- It might cause 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 pupil's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a child.

8. Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact- assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

9. Data Access Requests (Subject Access Requests):

Any individual, whose data is held by us, has a legal right to request access to such data or information about what is held. In all cases the DPO must be informed.

We shall respond to such requests within 1 month and they should be made in writing to:

Mrs T Bass (Head teacher)
Bushfield Road Infant School
Bushfield Road
Scunthorpe
DN16 1NA

When responding to requests the school will:

- Ask individuals to provide identification
- Contact the individual to confirm the request was made
- Respond within 1 month of the request
- Provide the information free of charge
- Inform the individual, compliance will be within 3 months of the request, where requests are multiple or complex – with an explanation as to why the extension is necessary.

If the request is unfounded, excessive, asks for further copies of the same information or repetitive we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

If a request is refused, the individual will be informed as to the reasons why and they will be informed that they have the right to complain to the ICO.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:-

• **Other schools**
If a pupil transfers from Bushfield Road Infant School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

• **Examination authorities**
This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

• **Health authorities**
As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and courts**
If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social workers and support agencies**
In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational division**
Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

10. Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

11. Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.
Written consent must be obtained from parents/carers for photographs and videos to be taken of their chid for communication. It must be clearly explained to both the parent/carer and pupil how the photograph and/or video will be used.
The use of photograph and video may include:

- The school website
- Within school on display boards
- School newsletters
- External agencies such as the school photographer or newspapers

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

When using photographs and videos in this way, they will not be accompanied with any other personal information about the child to ensure that they cannot be identified.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent and any images will not be shared on social media.

12. Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard.

Medical information that may require immediate access during the school day. This is stored within a locked cupboard in the school's medical room.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:-

• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

• Unwanted paper copies of data, sensitive information or pupil files should be disposed of in the school's confidential bin, which will then subsequently be shredded by the school's disposal management system. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

• If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

• If working at home, or off the school premises, school information should be accessed using staff Microsoft Office 365 accounts. Staff will use these accounts for email and other admin purposes using their own personal log in and password.

If it is necessary to transport data away from the school, it should be downloaded onto a USB stick or transferred using Office 365. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB on staff laptops, and saved onto the USB only. USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

1. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/
documents/1570/it_asset_disposal_for_organisations.pdf

The school has an identified qualified source for disposal of IT assets and collections as recommended by ACS. The school also uses Shred-it-all to dispose of sensitive data that is no longer required.

13. Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Head Teacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

14. Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or a room with restricted access.

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.

Confidential paper records will not be left unattended or in clear view anywhere with general access, such as left on office desks, classroom desks, staffroom tables or pinned to notice boards/ display boards

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

All electronic devices are password-protected to protect the information on the device in case of theft. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

When sending confidential information by email, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The recipient of the data has been outlined in a privacy notice.

Bushfield Road Infant School takes its duties under the GDPR very seriously and any unauthorised disclosure may result in disciplinary action. The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

1. Data Retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be safely disposed of, and

electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

2. Management of School Records

The school recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the overall management of the school.
This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

Staff must ensure that records for which they are responsible are accurate, maintained and disposed of in accordance with the school's guidelines.

Records are defined as those documents which facilitate the business carried out by the school and which may be retained for a set period to provide evidence of its transactions and activities. These records may be created, received or maintained in hard copy or electronically.

Pupil Records

These guidelines are intended to help provide consistency of practice in the way in which pupil records are managed. These assist schools by showing how pupil records should be managed and what kind of information should be maintained in the school.

Managing Pupil Records

The pupil record is seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file).

Recording information

A pupil or their nominated representative have the legal right to see their file at any point during their education and even until the record is destroyed (when the pupil is 25 years of age or 35 years from date of closure for pupils with special educational needs). This is their right of subject access under the Data Protection Act 1998. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

A Data Collection Sheet is created for each new pupil as they begin school and includes the following information so that it is easily accessible. This information is kept securely in a locked cupboard and includes:-

- Surname
- Forename and Middle name
- Chosen name
- DOB
- Address
- Gender
- The name of the pupil's doctor Emergency contact details
- Ethnic origin [although this is "sensitive" data under the GDPR 2018, the Department for Education require statistics about ethnicity]
- First Language (if other than English)
- Religion [although this is "sensitive" data under the GDPR 2018, the school has good reasons for collecting the information]
- Any allergies or other medical conditions that it is important to be aware of [although this is "sensitive" data under the GDPR 2018, the school has good reasons for collecting the information]
- Names of parents and/or guardians with home address and telephone number (and any additional relevant carers and their relationship to the child)

It is essential that these files, which contain personal information, are managed against the information security guidelines.

Items which should be included on the pupil record and retained securely (although these items may spread across more than one file):

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file (Teacher Assessment Files)
- Admission form (application form)
- Any notification of any pupil being admitted to the school in accordance with the North Lincs Fair Access Protocol (June 2019)
- Parental permission for photographs to be taken/not taken (Pupil Record of Achievement)
- Annual Written Report to Parents (Pupil Record of Achievement)
- National Curriculum Record Sheets (Teacher Assessment Files)
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child (Pupil Profiles)
- Any information about an EHCP and support offered in relation to the EHCP (SEND files)

- Any relevant medical information/Medical Care Plans (SEND files)
- Child protection reports/disclosures (CPOMs)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil.

The following records will also be stored separately as they are subject to shorter retention periods.

- Absence notes
- Annual Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues (Pupil Profiles)
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Transferring the pupil record to the junior school

Schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. The school does retain 'Pupil profiles' in the event of any subsequent legal action made against the school after the pupil has left. Custody of and responsibility for other records passes to the school the pupil transfers to.

All end of Key Stage One assessments are sent electronically to the junior school using their preferred format. These are sent via a secure NorthLincs e-mail to the Junior School's admin address. SEND files are delivered by hand to the junior school and signed for upon receipt by the receiving school for tracking and auditing purposes.

If files are sent by post, they should be sent by registered post with an accompanying list of the files. Where possible, the receiving school should sign a copy of the list to say that they have received the files and return that to our school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.

Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age (or the school where the pupil completed sixth form studies) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday.

Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the safe disposal of records guidelines.

Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact the Local Education Authority for further advice.

Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security. Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

1. **DBS data**

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

2. **Training**

All staff and Governors will be provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development.

Appendix 1:
Personal data breach procedure (Guidance from the ICO):

- The GDPR (May 2018) introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individual.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- *access by an unauthorised third party;*
- *deliberate or accidental action (or inaction) by a controller or processor;*
- *sending personal data to an incorrect recipient;*
- *computing devices containing personal data being lost or stolen;*
- *alteration of personal data without permission; and*
- *loss of availability of personal data.*

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft GDPR guidance on contracts and liabilities between controllers and processors.

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see our pages on reporting a breach.

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the

Article 29 Working Party guidance on identifying your lead authority.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What else should we take into account?

The following aren't specific GDPR requirements, but you may need to take them into account when you've experienced a breach.
It is important to be aware that you may have additional notification obligations under other laws if you experience a personal data breach. For example:

- If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our pages on PECR for more details.
- If you are a UK trust service provider, you must notify the ICO of a security breach, which may include a personal data breach, within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. Where this includes a personal data breach you can use our eIDAS breach notification form or the GDPR breach-reporting process. However, if you report it to us under the GDPR, this still must be done within 24 hours. Please read our Guide to eIDAS for more information.
- If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the NIS Directive. These are separate from personal data breach notification under the GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. You should look out for any such future guidance. Likewise, you should be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary detail.

Policy written: September 2019

Policy to be reviewed: September 2020

Policy approved by Governors: Autumn 2019