**Whitgreave Primary School**
**Procedure for Data Breach**

The General Data Protection Regulations introduces a duty to report certain types of data breach to the relevant supervisory authority (Information Commissioner's Office), and in some cases to the individuals affected.

A data breach is a breach of security leading to one or more of the following impacts on personal data:

- **Destruction of data (accidental of wilful intent)**
  This includes the deletion of electronic data

- **Loss of data**
  This can include, theft from Whitgreave Primary, theft from an employee's or Governor's car or home, data on a laptop that is lost or stolen, lost in the post, an email that is not received by the intended recipient. Loss can be internal to the Primary e.g. missing or mislaid files

- **Alteration of data (accidental or wilful intent)**

- **Unauthorised disclosure (accidental or wilful intent)**
  This can include data intentionally given to someone who has not right or need to have the data whether in hard copy, electronic format or by email, emails sent to the wrong email account, letters sent to the wrong address, information given over the telephone to a person who has no right or need to have the data, information given to a person during a conversation or in a meeting who has no right or need to have the data

- **Unauthorised access (wilful intent or inadequate protection)**
  This includes the wilful intent of a person to obtain information which they know they should not access, the disclosure of data because of the ability of a person who is given access by Whitgreave Primary to see data that they have no right or need to see due to inadequate safeguards being in place to protect that data, e.g. unlocked cupboards, general files, electronic systems with no password control.

All staff have a responsibility to report any instances or potential risks of data breaches at the earliest opportunity to the Data Protection Officer (DPO). The Data Breach notification form should be completed as soon as possible. It is not necessary

for this form to be completed before the DPO is notified on the breach as it is important that the DPO be notified of the breach at the earliest opportunity.

Data breaches can be either internal (data shared inappropriately within the Whitgreave Primary staff group) or external (data inappropriately released to other organisations/people, outside of Whitgreave Primary)

If a data breach is identified the Data Protection Officer should be immediately notified.

Internal breach

Should staff become aware that data has been inappropriately shared within Whitgreave Primary they should immediately notify the Data Protection Officer.

Such notification will enable all data incidents (including near misses) to be recorded and processes/procedures assessed and, where appropriate, updated.

External breach

Should staff become aware that data has been inappropriately shared with external organisations or people not employed by Whitgreave Primary they should immediately notify the Data Protection Officer.

The Data Protection Officer will notify the ICO of the data breach within 72 hours of receiving the notification if it is considered to have caused a potential risk to "the rights and freedoms of individuals".

The "72- hour clock" starts as soon as:

- An employee realises they have caused a breach and tells someone else (officially or unofficially)
- Another employee identifies there has been a breach
- The data subject informs Whitgreave Primary they have become aware of a breach by the Primary
- A third part informs Whitgreave Primary that there has been a breach caused by the Primary

Examples of potential risks/significant detrimental effects are:

- Discrimination
- Damage to reputation
- Financial loss
- Identify theft
- Confidentiality is broken
- Other significant economic or social disadvantage.

It is important to accept that what may not appear significant to Whitgreave Primary may be significant to an individual. The impact, therefore, must be assessed on a case by case basis, taking into account a person's personal circumstances.

**Notification to Information Commissioner's Office (ICO)**

On receipt of a data breach notification the DPO will contact the ICO by telephone providing basic details of the breach. This should be confirmed via email.

Following investigation, the DPO will confirm the following to the ICO:

- Nature of the breach
- The number of individuals affected by the breach and their relationship to Whitgreave Primary, e.g. pupils, parents, employees
- The number of records involved and the type of record e.g. one paper-based employee file, one electronic pupil file, single letter to parent re SEN, 35 SEN records
- Description of the likely consequences of the breach
- Description of the measures taken, or proposed to be taken, to deal with the breach
- Description of the measures taken to mitigate and possible adverse effects
- The name and contact details of the DPO

**Notification to the individual**

Following advice from the ICO the DPO will contact those affected.

If the numbers involved are small, the DPO will contact individuals directly to inform them of the breach, what action is being taken, any action required by the individual e.g. change passwords, inform banks etc.

If a large number of people are affected the DPO will make contact by sending a general message to those affected advising of the incident and any precaution they may need to take if they are concerned. This can then be followed up with direct contact once it has been ascertained exactly who has been affected and how.

It is an offence to omit notifying the ICO of an external data breach and may result in Whitgreave Primary being fined and/or an audit of the Primary's Data Protection governance arrangements