LIMPSFIELD GRANGE SCHOOL

'together we make a difference'

Data Breach Policy

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Governor's Committee Responsibility:	**Resources**
Date Approved:	**8th June 2018**
Review Period:	**3 yearly**
Next Review Date:	**Autumn 2021**

The Limpsfield Grange Values:

At Limpsfield Grange we believe in working together to make a difference.

We are a tolerant community; we accept, value and understand others.

We care for all members of our community without judgement.

We are responsible for our own learning, behaviour and actions.

We accept that sometimes things go wrong. We work together to take responsibility for our mistakes and for putting things right.

We are a respectful community and we treat others as we would like to be treated, even if they have different views and opinions to our own.

We understand that good behaviour helps us to prepare for life beyond Limpsfield Grange.

We are positive and resilient. We celebrate difference in everything that we do.

We are all proud to be part of the Limpsfield Grange community.

July 2017

Limpsfield Grange School – Data Breach Policy

Background and rationale

The General Data Protection Regulation (GDPR) (2018) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

All school staff will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Aims of the policy

This policy aims to inform staff Governors and other professionals working the school of their responsibilities regarding data breaches.

Scope

This policy applies to all staff and Governors of Limpsfield Grange, including members of our Outreach Service, and professionals working with students or staff at Limspfield Grange and professionals who have been commissioned by the school to provide the school with a service.

Definitions

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special category data

Previously termed “Sensitive Personal Data”, Special Category Data is similar by definition and refers to data concerning an individual’s racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Personal data breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Data Subject
The data subject is the person to whom the personal data relates.

Data Processor
Person(s) processing personal data on behalf of the Data Controller

ICO
ICO is the Information Commissioner’s Office, the UK’s independent regulator for data protection and information.

Responsibility
The School Business Manager has overall responsibility for breach notification within Limpsfield Grange. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the School Business Manager, please contact the Headteacher.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO’s contact details are set out below: -

Data Protection Officer: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

Security and data related policies
Staff should refer to the following policies that are related to this data protection policy:

- Security Policy which sets out the Limpsfield Grange’s guidelines and processes on keeping personal data secure against loss and misuse.
- Data Protection Policy which sets out the Limpsfield Grange’s obligations under GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found on the school website and on the adveryone drive.

Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it

When does a personal data breach need to be reported?

Limpsfield Grange School must notify the Information Commissioners Office of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- potential or actual discrimination
- potential or actual financial loss
- potential or actual loss of confidentiality
- risk to physical safety or reputation
- exposure to identity theft (for example through the release of non-public identifiers such as passport details)
- the exposure of the private aspect of a person's life becoming known by others

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting a data breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a data breach report form (Appendix 1)
- Email the completed form to the School Business Manager finance@limpsfield-grange.surrey.sch.uk
- Notify the Headteacher that a data breach has taken place

Breach reporting is encouraged throughout Limpsfield Grange and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, School Business Manager or the Data Protection Officer.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The School Business Manager will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the Data Protection Officer

Managing and recording the breach
On being notified of a suspected personal data breach, the School Business Manager will notify the Data Protection Officer. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in the School's data breach register
- Notify the Information Commissioner's Office
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breach.

Notifying the ICO
The School Business Manager will notify the Information Commissioner's Office when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the Information Commissioner's Office.

Notifying Data Subjects
Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the School Business Manager will notify the affected individuals without undue delay including the name and contact details of the Data Protection Officer and Information Commissioner's Office, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the School Business Manager will co-operate with and seek guidance from the Data Protection Officer, the Information Commissioner's Office and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

Notifying other authorities
The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers
- Parents

- Third parties (for example when they are also affected by the breach)
- The Local Authority
- The police (for example if the breach involved theft of equipment or data)

This list is non-exhaustive.

Assessing the breach
Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the Information Commissioner's Office and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is
- The volume of data affected
- Who is affected by the breach (i.e. the categories and number of people involved)
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise
- Are there any protections in place to secure the data (for example, encryption, password protection)
- What has happened to the data
- What could the data tell a third party about the data subject
- What are the likely consequences of the personal data breach on the school
- Any other wider consequences which may be applicable

Preventing future breaches
Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it is necessary to conduct a privacy or data protection impact assessment
- Consider whether further audits or data protection steps need to be taken
- Update the data breach register
- Debrief Governors following the investigation
- Any trends identified from data breaches each term will be discussed at termly Resources Committee Meetings.

Reporting data protection concerns

Prevention is always better than dealing with data protection as an afterthought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the School Business Manager or the Data Protection Officer. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Monitoring

This policy will be monitored by the Resources committee of the Governing Body who will receive updates regarding data breaches from the School Business Manager and the Headteacher.

Related policies

Staff should refer to the following policies that are related to this data protection policy: -

- Data retention policy
- Data protection policy
- Security policy
- Safeguarding Policy
- Staff Behaviour Policy

These policies are also designed to protect personal data and can be found on the school website.

Links

https://ico.org.uk/for-organisations/education/

Review

The Governing Body of Limpsfield Grange School adopted this policy on: ______________________

It will be reviewed on: ______________________

Signed ______________________

Dated ______________________

Appendix 1

Data Breach Reporting Form

Summary of Incident	
Date and time of incident	
Number of people whose data is affected	
Nature of breach, e.g. theft/disclosed in error/technical problems	
Description of how breach occurred	
Reporting	
When was the breach reported?	
How did you become aware of the breach?	
Who has been informed? ICO/LA etc.	
Personal data	
Full details of personal data involved (without identifiers)	
Number of individuals affected	
Have all affected individuals been informed?	
If not, why not?	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so please give details.	

Data retrieval	
What immediate remedial action was taken?	
Has the data been retrieved or deleted? If yes date and time	
Impact	
Describe the risk of harm to the individual as a result of this incident.	
Describe the risk of identity fraud as a result of this incident	
Have you received a formal complaint from any individual affected by this breach? If so give details	
Management	
Do you consider that the employee(s) involved has breached information governance policies and procedures?	
Please inform of any disciplinary action taken in relation to the employee(s) involved	
Had the employee(s) completed data protection training?	
As a result of this incident do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so what steps have been taken to address this?	
Has there been any media coverage of the incident? If so please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure	

Name………………………………………………………………………….. Signature…………………………………………………………….

Date…………………………………………………………………………….