LIMPSFIELD GRANGE SCHOOL

'together we make a difference'

Information Security 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:	**Autumn 2021**
Review Period:	**3 yearly**
Next Review Date:	**Autumn 2024**

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 – Information Security Policy

Background and rationale

The General Data Protection Regulations (GDPR) 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.

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Members of staff should refer to the School's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found in the school's adeveryone drive and on the school website.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

Aims of the policy

Limpsfield Grange School is dedicated to ensuring the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents sets out the measures taken by the school to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at Limpsfield Grange of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Limpsfield Grange School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, Governors and all third parties authorised to use our IT systems.

All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedures up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. 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.

General principles

- All data stored on our IT systems is to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.
- Members of staff should discuss with the School Business Manager the appropriate security arrangements for the type of information they access in the course of their work.
- All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.
- All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by either SoftEgg (general systems) or Babcock 4S (SIMS/FMS).
- The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with external providers (SoftEgg, StrictlyEducation4S, Capita)
- All members of staff have an obligation to report actual and potential data protection compliance failures to the School Business Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer:

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

Physical security and procedures

- Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when desks are left unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.
- The locked archive store shall be used to store paper records when not in use.
- Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, on the photocopier or printers, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. Particular care must be taken if documents have to be taken out of school.
- The physical security of buildings and storage systems shall be reviewed on a regular basis. Any issues with security must be reported to the Premises Manager or School Business Manager as soon as possible
- We have an intercom system and keypads on all external doors to minimise the risk of unauthorised people from entering the school premises.
- We close the school gates out of school hours to prevent unauthorised access to the building and monitor use of the gates throughout the day. The main school building and classrooms are alarmed and CCTV Cameras are in use around the school and in the grounds, these are monitored by the Premise Manager.
- Visitors are required to sign in at the reception, and pink badge visitors accompanied at all times by a member of staff. No visitors should ever be left alone in areas where they could have access to confidential information.

Computers and IT

SoftEgg in conjunction with the School Business Manager shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with Limpsfield Grange's security requirements;
- ensuring that IT Security standards within the school are effectively implemented and regularly reviewed, working in consultation with the Senior Leadership Team and Student Support Lead.
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

The School Leadership Team will be responsible for the following:

- ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.
- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems.
- ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;.
- receiving and handling all reports relating to IT Security matters and taking appropriate action in response (including, in the event that any reports relate to personal data, informing the Data Protection Officer).
- taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff.
- monitoring all IT security within Limpsfield Grange and taking all necessary action to implement this policy and any changes made to this policy in the future

Responsibilities – Members of staff

- All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.
- Computers and other electronic devices should be locked when not in use to minimise accidental loss or disclosure.
- The School Business Manager must immediately be informed of any security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.
- Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to SoftEgg as soon as possible.
- No personal software may be installed without the approval of the School Business Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
- All software must be installed by SoftEgg.
- Any virus must be reported immediately to the School Business Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Limpsfield Grange School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and protects our network. We also teach individuals about e-safety to ensure everyone is aware of how to protect our network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode.

- Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team.
- Members of staff should notify SoftEgg of any forgotten passwords to have access to the IT Systems restored. A new password must be set up immediately upon the restoration of access to the IT Systems.
- Passwords should not be written down if it is possible to remember them. If it is necessary to write down passwords then they must be stored securely (e.g. in a locked drawer).
- Passwords should never be left on display for others to see.

Members of staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data security

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the School Business Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems by SoftEgg.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School policies (including, but not limited to, this policy).

Electronic storage of data

- All portable data, and in particular personal data, should be stored on a password protected, encrypted memory stick or hard drive.
- All data stored electronically on physical media (USB, external hard-drive etc.), and in particular personal data, should be stored securely in a locked box, drawer, cabinet or similar.
- No personal data should be stored on any mobile device, whether such device belongs to Limpsfield Grange or otherwise without prior approval from a member of the Senior Leadership Team. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the school's computer network in order for it to be backed up.
- All electronic data must be securely backed up by the end of the each working day, this is completed automatically by SoftEgg.

Home working

Staff should not take confidential or other information home without prior permission of the Headteacher and only do so where satisfied appropriate technical and practical measures are in place within their home to maintain the continued security and confidentiality of that information.

Once permission has been given to take confidential or other information home, members of staff must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

Communications, transfer, internet and email use

- When using the School's IT Systems all staff are subject to and must comply with our Electronic Information and Communication Systems Policy.
- As a school we work hard to ensure our systems protect students and staff, and are reviewed and improved regularly.
- If staff or students discover unsuitable sites or any material which would be unsuitable, this should be reported to the School Business Manager.
- Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence. Any online safety breaches are discussed weekly at Senior Leadership Team meetings.
- All personal information, and in particular sensitive personal information and confidential information should be encrypted using Egress Switch before being sent by email, or sent by recorded delivery. Such information must not be sent by fax unless the sender can be sure that it will not be inappropriately intercepted at the recipient fax machine.
- Postal, fax and email addresses and numbers should be checked and verified before information is sent. In particular extra care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.
- All members of staff must be careful about maintaining confidentiality when speaking in public places.
- Confidential information should be marked 'confidential' and only circulated to those who need to know the information in the course of their work for Limpsfield Grange.
- Personal or confidential information should not be removed from the school without prior permission from a member of the Senior Leadership Team except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:
    - transported in see-through or other un-secured bags or cases;
    - not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
    - not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

- All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the School Business Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.
- When receiving a question or notification of a breach, the School Business Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.
- Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the School Business Manager.
- Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the School Business Manager.
- All IT security breaches shall be fully documented.
- Full details on how to notify of data breaches are set out in our Data Breach Policy.

Monitoring
This policy will be monitored by the Resources Committee of the Governing Body and the Senior Leadership Team.

Related Policies
Staff should refer to the following policies that are related to this Information (Data) Security Policy:

- Data Breach Policy
- Data Protection Policy
- Data Retention Policy
- Safeguarding Policy
- Staff Behaviour Policy
- Electronic Data and Communications 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	