LONDON BOROUGH OF HAVERING

ST. URSULA'S CATHOLIC PRIMARY SCHOOL

INFORMATION SECURITY POLICY

If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies page on the website for the latest update.

Controlled Document

Title	Information Security Policy
Document Type	For Approval
Author	Data Protection Officer
Owner	Headteacher
Subject	Information Security
Government Security Classification	Official
Document Version	Version 2
Created	September 2020
Approved by	Board of Governors
Review Date	September 2022 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control:

Version	Date	Author	Description of Change
1	29/12/2019	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	New Policy
2	21/09/2020	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review

Contents:

1. POLICY STATEMENT

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

St. Ursula's Catholic Primary School (hereinafter referred to as 'the School') is dedicated to ensuring the protection of all information assets within the keeping of the School.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

The School will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information security policy within the school including the supporting guidance documents which are listed below.

This Policy 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 the School Data Protection Policy in ensuring all staff are aware of and comply with UK law and School procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility for staff to protect the confidentiality and integrity of the information that they process.

2. INTRODUCTION

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

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

3. PURPOSE

Information is a major asset that the School has a responsibility and requirement to protect. The secure running of the School is dependent on information being held safely and securely.

Information used by the School exists in many forms and this policy includes the protection of information stored electronically, transmitted across networks and printed

or written on paper. It also includes any information assets in Cyberspace (The Cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services".

Protecting personal information is a legal requirement under Data Protection Law.

The School must ensure that it can provide appropriate assurances to its pupils, parents and staff about the way that it looks after information ensuring that their privacy is protected, and their personal information is handled professionally.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the School maintains, it also addresses who has access to that information, the processes they follow, and the physical computer equipment used to access them.

This policy details the basic requirements and responsibilities for the proper management of information assets.

4. SCOPE

This Information Security Policy and associated guidance documents, as listed below, apply to all systems, written, spoken and electronic information held, used or transmitted by or on behalf of the 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, contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems. All members of staff are required to familiarise themselves with its content and comply with 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 Procedure 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 and school processes that make up the School's information systems. This includes all Governors, school staff and agents of the School who have access to Information Systems or information used for school purposes.

5. GENERAL PRINCIPLES

All data stored on School IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information).

All data so classified must be handled appropriately in accordance with its classification.

All data stored on School IT Systems or 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 IT Consultant or by such third party/parties as the Headteacher may authorise.

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 the Headteacher unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the School Data Protection Officer who shall investigate the breach.

6. RISKS

The School recognises that there are risks associated with users accessing and handling information in order to conduct official school business.

The School is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the School to use all reasonable, practical and cost-effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure
- The confidentiality of information will be assured
- The integrity and quality of information will be maintained
- Authorised staff, when required, will have access to relevant school systems and information
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to staff on request

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and embarrassment.

7. 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 you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked filing cabinets and locked cupboards 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, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Headteacher as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

CCTV Cameras are in use at the School and monitored by Office Staff.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

8. ROLES AND RESPONSIBILITIES

It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the School's responsibility to ensure the security of their information, ICT assets and data. All members of the School have a role to play in information security.

The Headteacher in conjunction with the Senior Leadership Team and IT consultant shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;

b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;

c) 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.

Furthermore, the IT Consultant, in conjunction with the Headteacher and Senior Leadership Team shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;

b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;

c) 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;

d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relating to personal data, informing the Data Protection Officer];

e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;

f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and

g) 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.

All 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 the accidental loss or disclosure.

Staff must immediately inform the Data Protection Officer of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification 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 a member of the Senior Leadership Team immediately.

You are not entitled to install any software of your own without the approval of the Headteacher. Any software belonging to you must be approved by the Headteacher 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. Prior to installation of any software onto the IT Systems, you must obtain written permission by the Headteacher. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files. The Headteachers approval must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the IT Consultant and Data Protection Officer (this rule shall apply even where the anti-virus software automatically fixes the problem).

9. 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.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department. All passwords must, where the software, computer, or device allows:

a) be at least 6 characters long including numbers, letters and a special character (eg: $%£);

b) be changed on a regular basis;

c) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the IT Consultant as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password, you should notify the IT Consultant and a member of the Senior Leadership Team to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database).

Passwords should never be left on display for others to see. Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

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.

10. DATA SECURITY

Personal data sent over the school network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Headteacher 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.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the School's requirements and instructions governing this use. 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). The Headteacher may at any time request the immediate disconnection of any such devices without notice.

11. ELECTRONIC STORAGE OF DATA

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the IT Consultant.

No data to be stored electronically on physical media.

You should not store any personal data on any mobile device, whether such device belongs to the School.

Data may only be 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 and is done by Automated Processing.

12. HOME WORKING

You 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 your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

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

13. COMMUNICATIONS, TRANSFER, INTERNET AND EMAIL USE

When using the School's IT Systems, you are subject to and must comply with the School's Acceptable User Policy.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to a member of the Senior Leadership Team.

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.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission from the Headteacher 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:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g.in car boots, cafes, etc.)

14. REPORTING SECURITY BREACHES

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Data Protection Officer. 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 Data Protection Officer 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 Data Protection Officer. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Headteacher.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Data Protection Officer.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Security Incident and Data Breach Notification Policy.

15. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

16. LINKS WITH OTHER POLICIES

This information security policy is linked to the Schools:

- Data Protection Policy
- Freedom of Information Policy
- Security Incident and Data Breach Policy

- Acceptable Use Policy
- CCTV Policy

The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk