LLISWERRY HIGHSCHOOL

SCHOOL INFORMATION SECURITY POLICY

Owner:	**Mr I Roynon**
Updated:	**December 2020**
Next Review Date:	
Updated by:	**Mr I Roynon**
Governor Approval Date:	

School Information Security Policy

Created By:	**Newport Education Service**
Date Created:	**22 December 2009**
Version:	**V1.0**

Contents

Background

In order to ensure the efficient and effective delivery of school services we are making ever increasing use of Information and Communication Technology (ICT) and of pupil, financial and other information held by us, the local education authority (LEA) and other public sector organisations.

We recognise that the information we hold, process, maintain and share with others is an important asset and that, like other important business assets, needs to be suitably protected.

In order to build public confidence and ensure that the school complies with relevant statutory legislation, it is vital that we maintain the highest standards of information security; this Information Security policy sets out the school's approach.

GCSx is the **G**overnment **C**onnect **S**ecure e**X**tranet; a secure private Wide-Area Network (WAN) which enables secure communications between connected local authorities and other public sector organisations. To connect to this secure network, Newport City Council must comply with the key controls which have been defined by central government. As this school is connected to the Newport City Council network, with appropriate security configuration, we recognise that we are part of the overall secure network.

IT Infrastructure

a. The Council's IT Service will undertake technical separation of office and classroom machines from Council network and will undertake any necessary enhanced security on office machines.

b. The school's IT infrastructure will be maintained by the Lliswerry High School IT Support Team where all technical requirements can be discussed with the service providers and advice given as necessary.

IT Access

c. To ensure only appropriate users have access to school data the following safeguards will be in place:

- All users' passwords must be protected at all times.
- School Support Officers must use **strong**[1] passwords.
- School Support Officers' passwords will be changed at least every 90 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to school systems.
- Partner agencies or third party suppliers must not be given details of how to access the school's / Council's network without permission from IT Support.

[1] Strong (or complex) passwords contain a minimum of 8 digits, one each of UPPERCASE, lowercase, number, and 'special character (!"£$%^&*). Examples include **pA$$w0rd, Pro%F0otball, H0L!d4ys** (do not use these examples).

Acceptable use policy

d. All IT users agree to abide by an acceptable use policy, as this gives clarity to all parties regarding roles and responsibility of IT access and information/data usage.

e. The school's Acceptable Use Policy is reproduced at Appendix 1.

f. All staff and users will be periodically issued with a "Do and Don't Sheet" (Appendix 2) to enhance user education and awareness and to assist in reducing the possibility of a data breach within the school.

Email acceptable use

g. All emails that are used to conduct or support official school business must be sent using the school's official email system.

h. Non-work email accounts must not be used to conduct or support official school business.

i. Email correspondence which contains sensitive information will be encrypted before transmission to avoid a data breach should the email be mis-delivered.

j. Automatic forwarding of email must be considered carefully to prevent sensitive material being forwarded inappropriately.

Internet acceptable use

k. At the discretion of the Head Teacher, and provided it does not interfere with your work, the school permits personal use of the Internet in your own time (for example during your lunch-break).

l. Users are responsible for ensuring the security of their Internet account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.

m. Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.

n. Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

Sensitivity of data

o. The information that the school handles varies in levels of sensitivity. Appendix 3 sets out the sensitivity levels that the school has in place.

p. Level 1 information is deemed to be highly sensitive and mission critical information for limited consumption. In these cases the information will not be available beyond the school electronically.

q. Level 2 information is deemed to be essential to the successful running of the school, much of which can be accessed via the private side of the school's own learning platform. In these cases access to this information will be via personal logon which will be granted to only those users who need access to perform their duties.

r. Level 3 information is deemed to be generally within the public domain and accessed via the public facing website or learning platform. Minimum security will be afforded to this information as there is no risk of data breach.

s. Sensitive information deemed to be at levels 1 and 2 will not be held on personal laptops, computers or non-encrypted pen drives as the disposal and maintenance routes for these pieces of equipment cannot be controlled and may therefore leave sensitive school data at the risk of unauthorised disclosure / exposure.

t. The primary storage of all school data and information will be on the school network (curriculum or administrative network as appropriate) which is backed up daily and can be accessed remotely if necessary.

u. All sensitive information deemed to be at levels 1 and 2 will be disposed of securely when no longer required (whether paper or IT based).

Movement of data

v. It is recognised that the use of data pens and laptops leads to a higher risk of data breaches through the loss/theft of this equipment.

w. If data has to be moved from the school network then the movement must comply with the school's information sensitivity table (Appendix 3). In the case of information falling into Level 1 or 2 this will only be by the use of secure encrypted data pens; this will greatly reduce the risk of data loss / data breach should a device be mislaid.

Remote access to school's network

x. Remote access to the school's own network is available to all staff on the STEP system, and should be considered as standard for those needing to access school information and data beyond the school. This access negates the risk caused by removing data from school.

y. Remote access to school data by non-employees (including parents) will be carefully considered after consultation with the council's Education Service and STEP Team to ensure appropriate safeguards are in place that would not compromise the overall integrity of the school system. If this action is allowed then clear guidelines will be devised and shared with these groups to ensure safe and responsible use is maintained, with explicit sanctions published where safety is compromised.

Physical access to the school

z. It is recognised that a secure school and premises is also needed to support the overall security of school information.

aa. Visitors must always be signed in and escorted as necessary.

bb. All servers and associated control computers will be locked away and be accessible only to authorised staff.

Legal responsibilities

cc. The school will ensure compliance with the Data Protection Act 1998, Freedom of Information Act and other related information security statutory responsibilities.

Incident reporting

dd. Whilst every effort will be taken to ensure information security breaches or incidents do not occur, it is recognised that a clear incident reporting policy is necessary for the school.

ee. Security incidents can be summarised as:

- Theft or loss - of laptop, data pen, portable hard drive, Blackberry, sensitive information, remote access token, etc
- Malicious software (e.g. virus, spyware, malware, etc)
- Unauthorised access - to a PC/laptop or any school application (e.g. through personal password becoming known, leaving your work station unlocked when unattended, etc)
- Unauthorised access to the school building / office (e.g. break in or access to an unlocked and unattended room) which could lead to unauthorised access to the network or theft of equipment
- Impersonator trying to gain sensitive information held by the school that they are not entitled to (also known as social engineering)

ff. Should an incident occur the user will immediately report the facts to the Head Teacher who will arrange for the issue to be promptly investigated. A log of such incidents will be maintained and reviewed periodically to ensure that lessons are learned.

gg. The school will maintain an inventory of all ICT equipment, which will support the recording of loss or theft of any equipment or information.

Personnel processes

hh. Staff termination processes will ensure that all identification badges, keys and school equipment etc. are returned promptly for all leavers.

ii. All computer access will be promptly terminated on the user's last working day.

jj. Shared pass-codes (e.g. to secure door areas) will be changed after any member of staff leaves.

Linkages with other guidance

kk. The schools will also follow the Information Management Strategy from WAG, which provides practical advice and guidance in this important area.

ll. Furthermore, any local authority produced literature on this / related subject will be considered in full and, if appropriate review current procedures in line with recommendations.

Help and support

mm. It is understood that the local authority will provide E-safety guidance and a training pack for pupils, parents/carers and governors. The local authority has a number of accredited CEOP E-safety ambassadors who will also offer bespoke training sessions for these stakeholders.

nn. The local authority will also be available to offer help and support for any information security queries.

Policy compliance

oo. If any user is found to have breached this policy, they may be subject to investigation under the school's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Appendix 1 - Acceptable Use Policy (Lliswerry High School)

Lliswerry High School

The governing body have adopted Newport City Council School Information Security Policy. All staff must comply with the policy and sign an Acceptable Use Policy.

Acceptable Use Policy – Staff

The computer system is owned by the school. It may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management. This School's Acceptable Use Policy has been drawn up to protect all parties – the students, the staff and the school.

Computer Security and Data protection

I understand that:

- I must not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- I must not allow any student to use my personal login to any of the ICT systems for ANY reason.
- That pupils must not be allowed to use staff PCs
- I must take every reasonable precaution to secure any data or equipment removed from the school premises.
- That equipment taken off site will be my personal responsibility and I am advised to check that its loss or damage is covered by my personal insurance.
- I must not transmit any sensitive or personal information about staff or students via e-mail without data being encrypted by a method approved by the school.
- I must make your own backup of non-sensitive data kept on any storage system other than the network storage drives. This includes USB memory sticks or personal computer.
- I must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Laptops should be transported in a suitable laptop case.

Student protection

- I am aware of all guidelines to conceal student identities when publishing to the public domain
- I understand that students must be supervised at all times when in an ICT suite or on computer equipment
- When arranging use of ICT facilities I will ensure that a staff member is able to monitor pupils at all times
- I have read and understand my role regarding acceptable use and my role in enforcing it
- I will escalate noncompliance by students in accordance with school policy

Software, hardware, copyright and licensing

- I will not attempt to install any software or hardware
- **Before** purchasing any hardware or software I will consult a member of the IT Support staff to check compatibility, license compliance and discuss any other implications that the purchase may have
- I will respect copyright and make sure I do not use any information breaching copyright law
- Under **no** circumstances must any software from potentially illegal sources be installed
- I will not engage in activities that waste technical support time and resources.

Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- **must** comply with all other conditions of this Acceptable Use Policy as they apply to non-personal use, and all other school policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system.
- **must not** be for any commercial purpose or gain unless explicitly authorised by the school.
- You **must not** connect personal computer equipment or devices to school computer equipment or the network without prior approval from the IT Support staff, with the exception of storage devices such as USB memory sticks.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Use of E-Mail

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside of school. The following considerations must be made when communicating by e-mail:

- E-Mail has the same permanence and legal status as written hardcopy (paper) documents and maybe be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed by e-mail.
- E-Mail is not a secure method of communication, and can be easily copied, forwarded and achieved. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyright material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexual explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You **must not** send chain letters or unsolicited commercial e-mail (also known as SPAM)

Conduct

- You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
- You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet;
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using photocopiers.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook or MySpace, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You **must not** add a pupil to your ‘friends list’.
- You **must** ensure that personal information is not accessible via a ‘Public’ setting, but ensure it is set to a ‘Friends only’ level of visibility.
- You should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school’s reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Privacy

- Use of the school computer system, including your e-mail account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are not monitored or recorded.
- You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- Use of the school computer system indicates your consent to the above described monitoring taking place.

Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via the online Support Request system.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the IT Support staff, or the Headmistress, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

Reports should be made either via email or the online Support Desk system. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Declaration:

I have read the Newport City Council's School and Information Security Policy of Lliswerry High School and understand and will abide by these. I further understand that violation of the regulations is unethical. Should I commit any violation, my access may be revoked and I may be subject to disciplinary action.

User Signature: ____________________________________

Print Name: ____________________________________

Date: ____________________________________

Appendix 2 - Information Security "Do's and Don'ts"

"*Information security is about maintaining:*

- *Confidentiality - ensuring only people who have right to see the information can actually do so;*
- *Integrity - making sure that the information is right; and*
- *Availability - making sure that the information is always there when needed, and to the appropriate person."* WAG, 2008.

Do	Don't
• I agree to the most recently published schools Acceptable Use Policy and I accept that my use of the computer network and associated applications may be monitored and / or recorded for lawful purposes.	• I will not use a colleagues login details or share mine with anyone.
• I will lock my PC / laptop if temporarily leaving it unattended, by pressing <Windows> + <L>	• I will not leave a PC / laptop logged in and unattended.
• I will protect any sensitive material to the same level as paper copies including using a secure print option when materials are being printed a shared printer.	• I will not allow pupils to use a PC/laptop that is logged in with my username; I will always ensure that the student connects using their to personal credentials.
• Anything which needs to be shared will be shared through the teachers shared area(s), which may be password protected.	• I will not transfer any data which I know, or suspect, to have a high level of sensitivity, unless I need to and then only via an encrypted memory pen.
• I will always check that recipients of email messages are correct before I send it.	• I will not remove equipment from the school premises without appropriate approval.
• I will protect others from seeing sensitive information or me entering my password.	• I will not leave my password in a place which is easily accessed by others.
• I will report any e-safety incidents in line with the schools policy and procedures.	• I will not knowingly introduce a virus or other malware into the system.
• I will observe the schools Health and Safety policies and procedures.	• I will not disable anti-virus or malware protection provided on my machine.
• I will comply with the Data Protection Act and other statutory obligations.	
• I will ensure that any sensitive information is securely disposed of (whether paper or IT based). • I will immediately notify the loss or theft of any	
equipment or information in line with the School's Incident Reporting Policy. • I will sign out any portable device so there is a	
clear and up to date record maintained.	

Appendix 3 - Sensitivity of data

"*You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured*." Becta, 2009.

Level of sensitivity	Type of data	Possible level of protection
Level 1 Highly sensitive and mission critical information • for limited consumption.	• Child protection matters • Behaviour logs and discipline records Pupil personal information (UPN, name, address, DOB, phone etc.) • Staff personal information	• Not available beyond school electronically Encrypted with limited access to staff (SLT) when approved by HT.
Level 2 Essential to the successful running of the school, much of which can be accessed via the private side of the schools own learning platform.	• Attendance information & EWO reports • Performance Management information • Staff profiles and performance reviews • IEP's, AEN support, statements, annual reviews • Financial information	**Teacher access** • Login password • Limited to teacher ID • Password on specific files / folders **Pupil access** • Login only to their own progress records **Parent/carer access** • Login to own child records only (If applicable)
	• Pupil progress sheets • Examination data • Pupil reports • Letters to parents (specific issues) • Minutes of meetings (staff, dept., GB) • Performance of pupils • Rewards' records	
Level 3 Much is in the public domain and accessed via the public facing website or learning platform.	• Lesson plans, schemes of work • Teaching notes • School calendar, staff bulletins • School policies and procedures • Pupil work • Pupil learning logs • General school / class letters • Pupil photographs (parental consent)	• Pupil login • Password on specific files / folders

Level 2 has been split into two categories as many felt that some data in the top section may fall more appropriately under level 1. Accordingly, this data should be accessed remotely or, if being removed from school, the use of an encrypted pen may be more appropriate.

Appendix 4 – Student Acceptable Internet Use Statement

Lliswerry High School
Acceptable Internet Use Statement – Students

This document is to confirm that the holder of the user ID stated below is aware of the conditions of use of the Newport City Council/Lliswerry High School ICT system. On completion of this form a password for the ICT account will be issued.

Conditions of Use

I understand that in accepting a password to access the Newport City Council/Lliswerry High School ICT system, the following conditions of use apply:

- I must not share my password with anyone.
- I must not attempt to bypass any security within the system or alter the system or desktop.
- I must not use any other user's account or attempt to use someone else's password.
- I must not try to access unauthorised material. The Internet is provided as an educational resource and not to be used for games or social network websites.
- I must not store, access or transmit any material which is inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, homophobic or defamatory, infringes copyright or is unlawful.
- If I suspect that my access has been used by someone else, I must inform a system administrator immediately.
- I am responsible for logging off or suspending access to my last-used workstation whenever it is left unattended.
- I am responsible for the content of any stored material within my individual account.
- I understand that all my computer activity can be monitored at all times.
- I may only use the email facility of the school for school related activities.
- I should not copy and use material from the Internet to gain unfair advantage in my studies, for example in coursework (plagiarism).

Breaches of Conditions of Use

I further understand that if I should be suspected of having breached any of these conditions of use, then:-

- My computer access will be immediately suspended until an inquiry has been completed.
- If there is evidence of a breach of the conditions of use, then this will be regarded as very serious and that I will not be allowed access to the system for a fixed time or for more serious offences that I might be excluded from school.

Agreement

I have read and agree to abide by the conditions of use of the Newport City Council/Lliswerry High School ICT system and I am aware of the actions that will be taken if I breach these conditions.

User Signature: ____________________________________

Print Name: ____________________________________ **Form:** ______________

Date: ____________________________________

Appendix 5 – Laptop Use Policy

Laptop User Policy

Purpose of this document

- This document intends to outline the permitted uses of School laptops and accessories.
- All rules contained must be strictly followed. Breaching these rules may result in disciplinary action.

General information

- All laptops and accessories are on loan to staff whilst they are employed at the School.
- At no time is the laptop the personal property of any staff member. Laptops must be presented upon request and must be returned upon the staff member leaving the School's employ on last day of teaching.

Use of laptops

- All staff are reminded that staff wishing to use the laptops to store information, such as student or staff data, should only do so when it's essential, and under the guidance of the Data Protection Act 1988
- Laptops that are configured to use the School network may be connected to the School's data infrastructure using any 'live' data socket or a wireless connection (where available).
- The laptops will then have access to the full range of software and services, plus a default printer will be allocated.
- Laptops should be used within School at least once a month to receive software patches and antivirus updates. These will be performed automatically and will be transparent to the end user.
- An offline copy of any user files can be kept on the laptop. Files can be backed up to the school server using LHS Connector. These files will also be stored on the network for access in School or at home using Remote website and backed up following the School's standard backup regime. All laptops come preinstalled with an encrypted hard drive in the event of laptops being lost or stolen.

Illegal and suspect activity

Laptops must not be used for any illegal or suspect activity. This includes:

- The use of illegally obtained software – this is all software that does not have a valid license certificate
- Use of the laptop for questionable activity – including the deliberate viewing of inappropriate material on the Internet
- Actions that may contravene the Computer Misuse Act 1990

Agreement

I have read and agree to abide by the conditions of use of the Lliswerry High School laptops and I am aware of the actions that will be taken if I breach these conditions.

Full Name:		**Signature:**	
Department:		**Date:**	

For office use only:

Asset No:		**Serial No:**	
PC Name:		**MAC:**	
Make:		**Model:**	