St Mary's Catholic Primary School

Achieving Ambitions

INFORMATION AND ICT SECURITY POLICY

We guide our pupils on to the path to achieving their ambitions.

On their journey, they **Love** *one another,* **Learn** *to achieve excellence,* **Laugh** *through enriching experiences and* **Live** *life to the full.*

Drafted by	SLT and IT Technician
Approved by Governors	Not required
Reviewed	Autumn 2023
Next Reviewed	Autumn 2025

Information and ICT Security Policy

The objectives of this Policy are to:

Ensure the protection of confidentiality, integrity and availability of school information and assets.

Ensure users are aware of and fully comply with all relevant legislation.

Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

This policy relates to the following whole school policies and documents:

- Data Protection Policy
- Freedom of Information Publication Scheme
- Acceptable use Agreements for staff and pupils
- Child Protection & Safeguarding policies
- Online Safety policy
- Privacy Notices
- Cyber Response Plan

Legislation

St Mary's recognises the requirements of the current legislation relating to the use of ICT systems and information security, which comprise principally of:

*Copyright, Designs and Patents Act 1988
*Computer Misuse Act 1990
*Human Rights Act 1998
*Data Protection Act 1998
*Freedom of Information Act 2000
*General Data Protection Regulation (GDPR) 2018

Through briefings and training all staff will be kept aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

Scope

This Policy is intended for all school staff, including governors, who have control over or who use or support the school's administrative and/or curriculum ICT systems or data or handle other school manual (paper) and electronic data. All users of the school's ICT systems or data are also covered by this policy.

Policy Definitions

"Data" means information in any format, e.g. paper, electronic, video, audio.

"Authentication" means the process of identifying an individual, usually based on a username and password, i.e. determining whether someone is, in fact, who they claim to be.

"Personal data" means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

"Sensitive personal data" means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs or other beliefs of a similar nature, (d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) their physical or mental health or condition, (f) their sexual life, (g) the commission or alleged commission by them of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Responsibilities

• The Governing Body

The Governing Body has ultimate responsibility for ensuring that the school complies with the legislative requirements relating to the use of information and ICT security and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Head teacher.

• The Executive Head and Head of School

The EXH and HofS is responsible for ensuring that the legislative requirements relating to the use of information and ICT system security are met and that the school's Information Security and Acceptable Use Policy, as may be amended from time to time, is adopted and maintained by the school. The EXH and HofS is also responsible for ensuring the requirements of the Data Protection Act 1998 are complied with fully by the school. In addition, the EXH and HofS is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. (See checklist Appendix I)

• The Senior Information Risk Officer (SIRO)
The SIRO is a senior member of staff who is familiar with information risks and the school's response. The following responsibilities attach to the role of SIRO:

• They own the Cyber Attack Response Plan
• They act as an advocate for information risk management

Further details on the roles of responsibilities of the SIRO are in Appendix II

Managing Information Systems

How are the school's information systems' security maintained?

• The school's broadband network is protected by a cluster of high performance firewalls and filters at the Internet connecting nodes in Brighton & Hove. These appliances are monitored and maintained by ICT staff employed by Brighton & Hove City Council.

• The security of the school information systems and users will be reviewed regularly by the SIRO and IT Technician

• Virus protection will be updated regularly by the IT Technician in liaison with BHCC.

• Where we use Wireless LANs they will be configured for encryption of network traffic and with no broadcast to prevent unauthorized access to school data.

• Administrative PCs will not be accessible via wireless networking unless there is an approved managed wireless solution in place providing authenticated access to secure data.

• In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, a backup is automatically made each evening by the local authority using a secure connection to their servers. In addition appropriate processing controls such as audit trails can be requested from BHCC's ICT Department should the need arise.

How is password security managed?

All staff are issued with a network user account by the IT Technician which is protected with a password which is not to be shared. Sharing of passwords and accounts is a security breach and as there is no traceability of who did what on the network if a breach occurs. PC/devices must not be left unattended once logged in. If a device must be left unattended then it must be logged out or locked (Windows logo key +L). The use of user logins and strong passwords to access the school network, work email and the online calendar by staff will be enforced. Staff passwords must:

• Three random four letter words, where the first letter of each word is capitalised

• must NOT be shared with anyone else under any circumstances;

• will be locked out after six successive incorrect attempts;

Users are discouraged from saving passwords in any sort of web browser log on page. There are a set of guest accounts for use by supply teachers and student teachers. These allow green access to the network and ARBOR registration tutor access. Passwords of these are changed regularly to limit the risk of a previous supply teacher accessing the network when they should not.

How is data kept secure on the school's server?

The school's server is organised into folders that appear as mapped drives when a registered user logs in. Each drive has security settings that dictate which users have access and the type of access they have: none, read only, write only or read & write access. The level of access granted for each user is based on their security group membership. Only the IT Technician is able to create and edit user accounts and security groups. Access rights are granted by the SIRO in consultation with the Head teacher. Access eligibility will be reviewed continually, including remote access to systems and external web services. In particular the relevant access capability will be removed when a person leaves the employment of the school or their role changes. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties. All data stored on the school's servers is assessed as to its personal/sensitive nature using a colour coding system.

Red data (those that contain sensitive personal data)

Eg:
ILPs/Provision Maps
Education Psychologist reports
Education Welfare Officer reports
Medical records
Personnel records e.g. Addresses, Dates of Birth, Wages
SEN registers
SIMS data
Staff's "My Documents" folder

*Access to Child Protection data is limited to the Head teacher, Deputy Head and Deputy Designated Person.

Amber data (data that contains personal data that if lost could identify individuals)

Eg:
Names and Addresses
Parental contacts
PINs
Class/group lists with full names
Pupil reports including End of Year Reports
Teacher Assessments, SATs results etc.
*This data is only accessible by those on a "need to know" basis.

Green data (data that does not identify individuals)

Eg:
Lesson plans

Class lists (only showing initials or forenames)
Curriculum plans
General marking

If you don't mind it being available on a website or in the local paper then it is green data.

How will staff Internet access be authorised?

• The school has dual Internet filtering which allows staff to access online resources e.g. Google images, Youtube that are blocked to pupils. In order for staff to access this they must read, agree to and sign the "Relaxed Filtering" form which is forwarded to Schools ICT for processing.
• The school maintains a current record of all staff who are granted access to the school's electronic communications and at which level.
• All staff will read and sign the School's Acceptable Use Policy before using any school ICT resources.
• All visitors to the school site, including supply teachers and student teachers, who require access to the school's network or Internet access will be asked to read and sign an Acceptable Use Policy.
• When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

What constitutes a breach of legitimate use of the school's ICT resources?

The school's ICT facilities must not be used in any way that breaks the law or breaches local authority standards. Such breaches include, but are not limited to:

- Taking red data off the school premises.
- Taking amber data off the school premises unencrypted.
- Unauthorised access of another users account (computer, email, MIS etc)
- Using USB drives to take any data off the school premises.
- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, extremist or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised private use of the schools computer facilities;

How will staff send and receive email?

• Staff must use approved email accounts for school purposes.
• Staff emails are administrated by Schools ICT department (ictsts@brighton-hove.gov.uk)
• The use of email and attachments follows Brighton & Hove's guidelines.
• Staff can request email password reset from the SIRO or administration office
• Circular emails to parents and other stakeholders should be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone.
• Any email containing sensitive/personal information (as defined above) must only be sent using the local authority's encryption system by typing [encrypt] in the subject box.
• The forwarding of chain messages is not permitted.
• Push email (i.e. using an app to manage emails that does not require a password) to mobile devices will only be permitted after the member of staff has signed a contract and returned it to Schools ICT.

How will data taken off-site be managed?

• Sensitive and Personal data may only be taken off-site using encrypted* electronic modes i.e. laptop (where the entire drive is encrypted); using encrypted email or uploading to One Drive.
• The use of cloud storage e.g. DropBox, Google Drive, Skydrive must only be for green data as these are not covered by EU data law and have no virus scanning.
• The use of any centrally stored data, e.g. Target Tracker, may only be permitted with proof of data security from the company.
• Portable media may not be used without specific permission followed by an anti-virus / malware scan (right-click force scan by SOPHOS)
• Unapproved software is not allowed in work areas or attached to email.
• Files held on the school's network will be randomly checked by the SIRO for sensitivity and appropriateness of location/access.
• The ICT coordinator/technician will review system capacity regularly

How are images and video managed?

The school has a variety of cameras, tablets and other devices that can record images. Staff should be mindful that not all of these have the required encryption level of protection. Staff are reminded not to use any personal device to record images or video of pupils. Staff are encouraged to download images/video onto the network as soon as possible and delete them from the device. Where a school camera needs to be taken off-site i.e. sports fixture, educational visit, residential trip the memory card must be empty before leaving.

How are staff personal devices managed?

• Staff are not permitted to use their own telephones or devices for contacting children, young people and their families within or outside of the school in a professional capacity.

• Use of mobile phones within school is covered by the Staff Handbook.

• If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

• Personal mobile devices including smartphones and tablets must not be used to communicate (via phone, text or other messaging system) or make records of any kind (image, audio or video) in lessons by anyone, in line with the school's Safeguarding Policy.

• Use of mobile devices for other organisational apps e.g. calendar, notes, document access is acceptable as long as no personal or sensitive information is saved to the device.

• If a member of staff breaches the school policy then disciplinary action may be taken.

How is the physical security of information and electronic data managed?

Location Access

As part of the annual review of this policy consideration will be given to the physical security of rooms containing sensitive information and ICT equipment (including associated cabling). As far as practicable, only authorised persons will have access to the servers. The IT Technician will ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements will take into consideration the risks associated with the removal and the impact these risks might have. All school owned ICT equipment is recorded in the school's inventory and security-marked. Where appropriate we will seek advice from Brighton & Hove's Crime Prevention Officer as to best practice in this area. Where necessary we will use power supply protection from voltage surges to minimize the risk of servers failing. Uninterruptible Power Supply (UPS) units are used to ensure a controlled shutdown of servers and network cabinets should a power failure occur.

Paper Records

All information of a sensitive / personal nature must be stored securely.

• Staff's and pupils' records are stored in locked cabinets and rooms that are locked at night. Access to the keys is limited.
• Visitors are not left unattended near sensitive / personal data unless they are professionals invited to the school for specific purpose e.g. Social Services, Speech & Language therapist
• Pupils are not allowed in rooms without an adult.
• Assessment information is locked away at the end of day.
• A "clear desk policy" should be adopted, i.e. hard copies of sensitive/personal data are not left unattended on desks.
• Emergency medical information is displayed, with the permission of parents, out of view of the public e.g. pupil's risk of and response to anaphylaxis. This is to strike the balance between the need to inform of life threatening illnesses and the need for privacy.
• Disposal of all paper copies of sensitive/personal information is in line with the Disposal of Information and Retention Policy.

Use of staff personal PCs/laptops/devices at home

PCs/laptops that have stored or provide access to data can cause a security risk if they are not disposed of in a secure way meaning that sensitive or personal information could be available to anyone who comes into possession of the device. If school data is breached from staff's own PCs it is their own responsibility. It is important that if there is any school information stored on a personal PC/laptop/device then it must not be seen by anyone else including anyone else using the PC at alternative times. Separate user accounts should be set up where other people may access the device. Dispose of any personal computing equipment that has been used for school related work of a sensitive or personal nature (red or amber) must be in a secure manner ensuring that the machine is forensically wiped to CESG Infosec Level 5 HMG standards. It may be possible to dispose of personal PCs with school information on it when the school disposes of its own equipment if the school agrees.

Siting of Equipment and Information

All staff will be made aware that reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

• information (paper or electronic) should be protected in such a way that it cannot be accessed or viewed by persons not authorised to access it.
• devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved. PC/devices must not be left unattended once logged in. If a device must be left unattended then it must be logged out or locked (Windows logo key+L)

• equipment should be sited to avoid environmental damage from causes such as dust and heat.
• users should enable password protected screen savers to protect screen content if unauthorised access to the data held can be gained when left unattended. Information & ICT Security and Acceptable Use Policy
• network servers and infrastructure are located in an environment with the appropriate temperature and sufficient security.

These rules will also apply to school equipment in use at a user's home.

Disposal of assets

Records will be kept of all ICT assets disposed of and the measures taken to ensure protection of sensitive data. The SIRO must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed. The Local Authority's Procurement Framework will be utilised where necessary to dispose of redundant equipment in accordance with the WEEE directive. Storage devices being disposed of must be forensically wiped to CESG Infosec Level 5 HMG standards.

Risk Assessment

As recommended, the SIRO undertakes a thorough risk assessment on the information assets held. This helps to identify what security measures are already in place and whether they are the most appropriate (and cost effective) available. Carrying out an information risk assessment will generally involve:

• Recognizing which risks are present
• Judging the size of the risk(s)
• Prioritising the risks
• Once the risks have been assessed, a decision can be made on how to reduce them or accept them.
• Risk assessment is an on-going process and the school will review these at regular intervals as risks change over time.

Security Incidents

Any of the following security incidents must be reported to the SIRO and IT Technician, or the Headteacher in their absence, who will report the incident to the ICT Support Help Desk (01273 293663) or our *Data Protection Officer: James England.

These include;
• Any suspected or actual breaches of information or ICT security,
• Any detection of computer viruses or malware that may have been inadvertently download or copied to the school network,
• Any inappropriate use of a computer/device - do not turn off or allow anyone to access the computer/device as it may affect importance evidence,
• Loss of personal mobile phone if it was used to read school email,
• Theft of laptop or personal PC if used for school work (even if these devices were encrypted and no data was lost it is still good practice to report them to the school as “near misses”.)

*Please see Data Protection Policy

APPENDIX I

Headteacher/SIRO's checklist

This checklist is designed to assist Head teachers to ensure that personal information in either paper or electronic format is being managed appropriately. It is the Head teacher's responsibility to:

Check with staff if they take personal information or equipment away from school.	☐
Does personal information need to be taken off site?	☐
Is the amount of personal information leaving the school limited to that which is actually needed, i.e. data isn't left on memory sticks or laptops if it is not specifically required?	☐
Personal data isn't stored on memory sticks or laptops unless the devices are encrypted. The Information Commissioner's Office does not consider password only protection to be sufficient.	☐
When taken out of the school, personal information is going to be kept securely and access limited to the member of staff, either in transit or in the home environment.	☐
Is anti-virus software and operating system software (Windows/Mac) kept up to date? At a minimum staff must ensure that laptops are updated as soon as they are returned to school. [The Council has previously suffered a serious incident affecting the whole school network as a result of computer software not being kept up to date over a Summer break].	☐
If school computer equipment is being taken home, access to the computer is restricted to the member of staff's usage.	☐
Personal photographs, music, video, non-school software should not be stored on a school computer.	☐
Staff are aware that they should use the computer in the home environment as they would at school, in line with any school "appropriate usage" guidance.	☐
When the school is closed personal information and portable computer equipment remaining at school is secured out of sight.	☐

APPENDIX II

Roles & Responsibilities of the Senior Information Risk Office (SIRO)

The Senior Information Risk Officer (SIRO) is a senior member of staff who is familiar with information risks and the school's response. The following responsibilities attach to the role of SIRO:

- They own the Cyber Attack Response Plan
- They act as an advocate for information risk management

Additionally, the SIRO will be responsible for ensuring that:

• Suitable training for all users and documentation to promote the proper use of information and ICT systems is provided.
• Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data.
• A record of the training provided through the school to each individual user will be maintained.
• Users are made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for information and ICT security.
• The relevant parts of the Cyber Attack Response Plan, and any other information on the use of particular facilities and techniques to protect the systems or data, will be disseminated to users.

The SIRO will ensure that the practical aspects of ICT protection are performed, such as: maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

The SIRO has a responsibility for ICT equipment and systems and will have control over these assets and their use, including responsibility for controlling access to these assets and for defining and recording the requisite level of protection. In line with these responsibilities, the SIRO will be the official point of contact for ICT or information security issues and as such is responsible for notifying the Head teacher or Chair of Governors of any suspected or actual breach of ICT or information security occurring within the school. The SIRO or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to the Council's Information Governance team upon request. The SIRO or Chair of Governors must advise the ICT Support Help Desk (01273) 293663 or Data Protection Officer 0800 0862018 of any suspected or actual breach of ICT or information security immediately. It is vital, therefore, that the SIRO is fully conversant with the Cyber Attack Response Plan and maintains an up to date knowledge of best practice and follows the associated approved practices.

APPENDIX III

Acceptable Use Policy – Staff

Note: All internet and email activity is subject to monitoring

You must read this policy in conjunction with the online Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the online safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or child, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that information is kept securely and is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device and without being checked by the Headteacher or Assistant Headteacher.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher or Deputy Head who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and school staff.

Viruses and other malware - any virus outbreaks are to be reported to the Assistant Headteacher and ICT support team as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Online Safety – like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with children.

Email Phishing Attacks

SLT will never send emails asking you to purchase items without discussing with you first.
Any suspicious emails should automatically be reported to SLT or the IT Technicians

NAME :

SIGNATURE : **DATE :**

APPENDIX IV



Conditions for the use of relaxed, adult Internet filtering.

Please read the conditions below and indicate your agreement by signing this form and returning it to the e-Safety Coordinator or IT technician.

Please can you also confirm that you have received training about the relevant points below?

1. I will ensure that any video that has originated online must first be viewed by me, in its entirety before showing it to pupils. ☐
2. I will ensure that any computer that has been logged onto by me will be locked when not in use. ☐
3. I will not share my computer password with anybody. ☐
4. I will not allow anybody else (especially a pupil) to use a computer that has been accessed using my credentials. ☐

(Points 2-4 are all required practices under the Data Protection Act)

I confirm that I understand & agree with the points above. ☐

Print your name.....

Signature..... Date.....

APPENDIX V

Information required for creating Office 365 email and Wave4schools accounts

Please email back to ictsts@brighton-hove.gov.uk – preferably send your requests 2 weeks before the employment start date.

If you require an email and wave4schools account to be given to staff before the summer for their September start date:
we will need an email confirmation from your Headteacher that they accept responsibility for this – the staff account holder will need to sign your school acceptable use policy covering email accounts.

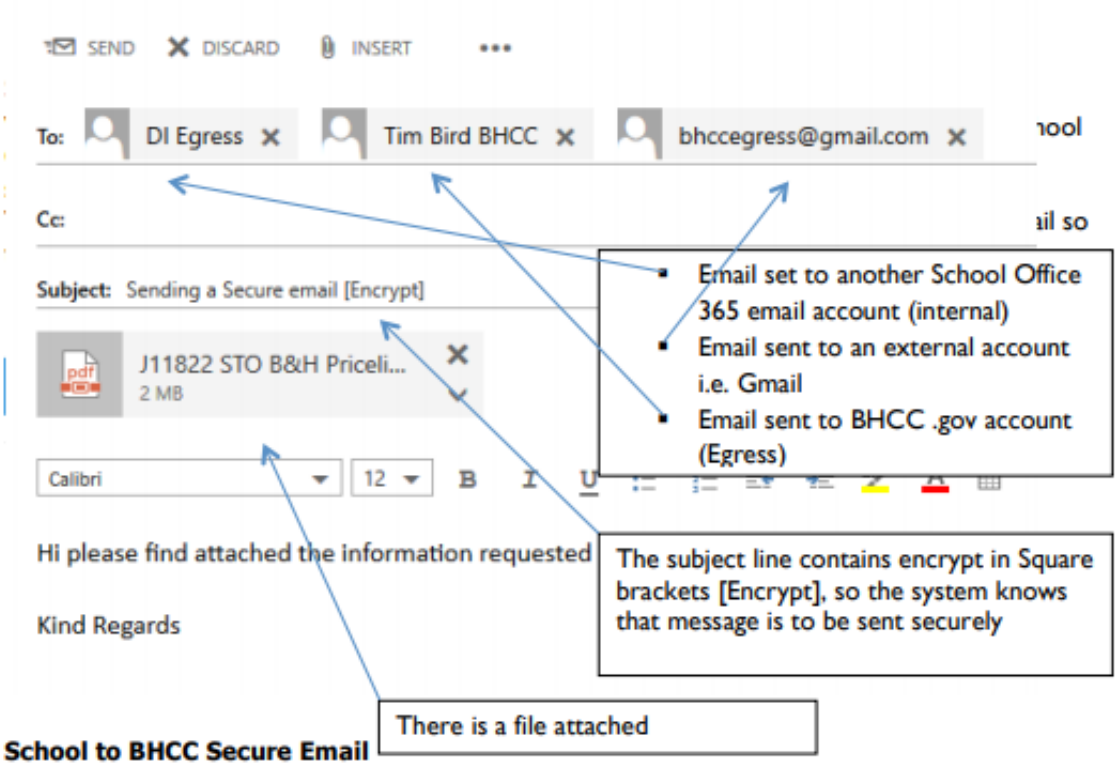
Please complete the appropriate section. You are welcome to add or delete the boxes as you need them.

How to send a secure encrypted email using Office 365

Method 1 – adding [Encrypt] to the body or subject of the message

All Office 365 email users for Brighton and Hove schools can now send, and receive Egress encrypted (secure) emails by simply adding [encrypt] anywhere in the email subject line or the body of the message.

Example :



School to BHCC Secure Email

When secure email is sent to and from schools to BHCC using Egress encrypted mail there is an orange header added to the message as it will be automatically decrypted as BHCC also has Egress installed.

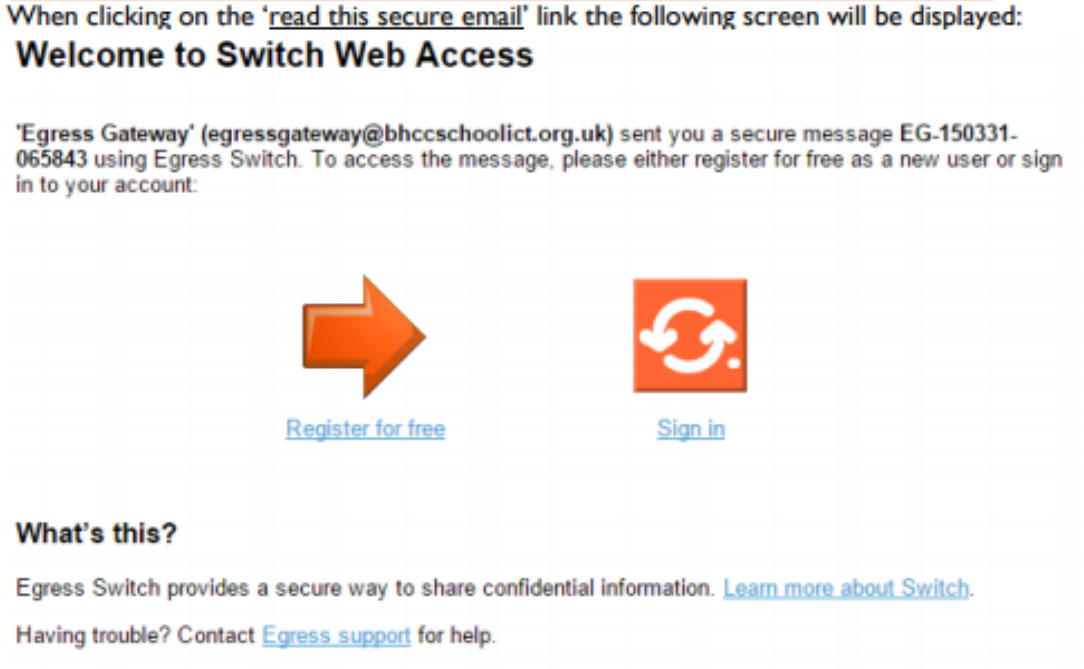


School to External Secure Email (Gmail ,Hotmail ,yahoo, BT etc.)

Secure encrypted mail can be sent to recipients outside BHCC, such as NHS staff or parents. The content of the secure encrypted message is only accessible through a secure online port. The recipient will see the following message appear in there inbox, informing them that they have been sent information in an encrypted email and stating what they need to do to access that information.



When clicking on the '<u>read this secure email</u>' link the following screen will be displayed:



The system will then take you through the registration process.