
St Mary & St Paul's CE Primary School

Online Safety Policy

Vision and Values

The school's vision and mission statement underpins the high standards of behaviour expected at all times at St Mary & St Paul's CE Primary.

'Life in all its fullness through Learning and Love'

This policy should be read in conjunction with the Anti-Bullying Policy, Behaviour Policy, Acceptable Use Policy and the Safeguarding & Child Protection Policy.

Online Safety is an important part of keeping children safe at St Mary & St Paul's CE Primary School. It covers all electronic media and we constantly strive to protect and educate our pupils in the digital world we live in. It is embedded into our school curriculum, particularly in Computing and PSHE lessons. Pupils are taught how to stay safe and behave appropriately online.

We aim to tackle any Online Safety issues by trying to prevent it from occurring in the first place, and by tackling it consistently, fairly and effectively whenever it does. We are committed to promoting a safe environment online where children can learn and play, as well as communicate sensibly, while also being aware of the risks and dangers.

At St Mary & St Paul's, we take pride in the teachings of our unique school values that underpin and promote the British fundamental values where British law, democracy and a mutual respect and tolerance for those of other faiths, cultures and beliefs is embedded through all areas of the curriculum. Pupils are encouraged to be independent learners, constantly making choices, within a safe and supportive environment. Developing their self-esteem and self- confidence is very important. Pupils are encouraged to understand their personal freedoms and are taught how to use these rights to best effect.

Areas of Risk

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Accessing social media sites inappropriate for primary aged children
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identify theft (including hacking social media profiles) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well being (amount of time spent online).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film)

(Ref Ofsted 2013)

The policy applies to all members of St Mary & St Paul's CE Primary School community (including staff, students, volunteers, parents/carers visitors, community users) who have access to and are users of school/ academy computer and communication systems, both in and out of St Mary & St Paul's CE Primary School.

Role and Responsibilities

Leadership Team

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community.
- The Leadership Team are responsible for ensuring that the Computing Subject Leader and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Leadership team should be trained in Online Safety issues and be aware of the potential child protection issues.
- The leadership team will liaise with school ICT technical staff and receive reports of Online Safety incidents and will log this information and use it to inform future Online Safety developments.

Computing Subject Leader:

As part of their role, the Computing Subject Leader will take day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing Online Safety policies/documents. In addition, they will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- promote an awareness and commitment to Online Safety
- ensure that Online Safety education is embedded across the curriculum.
- provide training and advice for staff and parents.
- liaise with the Local Authority and relevant staff in our Connect network group.
- liaise with school ICT technical staff and receive reports of Online Safety incidents. They will log this information and use it to inform future Online Safety developments.
- record and review all incidents relating to extremism in order to establish whether there are any patterns of extremist groups targeting the school and whether current procedures are robust enough to deal with the issue.

Local Authority:

It is the roles of the ICT team at the Local Authority to ensure that:

- reasonable systems are put in place to ensure that the network and related infrastructure is as secure as possible.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with Online Safety technical information in order to effectively carry out his Online Safety role and to inform and update others as relevant.
- equipment is protected adequately against threats such as hacking and viruses.
- the network infrastructure is monitored regularly and consistently.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school / academy Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement

- they report any suspected misuse or problem to the Headteacher / Senior Leader / Computing Coordinator for investigation /action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- e-mails sent to parents/guardians or any other agencies should be on a professional level and sent through maryandpaul@knowsley.gov.uk
- they are aware of those students who may be targeted or exposed to harmful influences from violent extremists via the internet. Students and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies. All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.

Governors

To enable the Governing Body to carry out its duties in promoting high standards of education and achievement, governors need to be fully informed about the standards in Online Safety as well as priorities for development. Governors are kept informed in the following ways:

- The Headteacher reports to governors termly on progress towards objectives within the school improvement plan.
- The governors are given the opportunity to approve the Online Safety Policy and review the effectiveness of the policy.

Safeguarding Designated Persons

Any safeguarding designated person should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.

•potential or actual incidents of grooming.

•cyber-bullying.

Parents

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of Computing than their children. The school will therefore take every opportunity to help parents understand these issues through the school website, parent evenings and newsletters. Parents may also invited to attend an annual Online Safety workshop.

Parents/Guardians will be responsible for:

•supporting the school in promoting Online Safety and endorsing the Parents' Acceptable Use Agreement (see Appendix 2) which includes the pupils' use of the Internet and the school's use of photographic and video images.

•reading, understanding and promoting the school Pupil Acceptable Use Agreement with their children.

•consulting with the school if they have concerns about their children's use of technology.

Pupils

It is important that all pupils at St Mary & St Paul's CE Primary school:

•have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

•need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

•will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

•should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's / academy's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

•Policy to be posted on the school website with hard copies available from school on request.

•Policy to be part of school induction pack for new staff.

•Acceptable use agreements discussed with pupils at the start of each year.

•Acceptable use agreements to be recorded by the office and kept in teacher files.

When using communication technologies the school considers the following as good practice:

•The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
•Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
•Any digital communication between staff and pupils (on iOS applications such as SeeSaw) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
•Students / pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
•Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approaches to Teaching and Learning

Online Safety is embedded into the curriculum and is covered through Computing and PSHE objectives.

Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Pupils will be expected to know school rules and understand school policies for bullying and behaviour, this is reinforced through circle time and Safer Internet Sessions each half term.

Pupils should understand the importance of adopting good Online Safety practice when using digital technologies out of school.

Handling complaints

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview with teacher/ Computing Subject Leaders/ SLT / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including online homework];
- Referral to LA / Police.

Our Computing Coordinators act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The Online Safety policy is referenced from within other school policies:

- The school has Computing and PSHE subject leaders who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online Safety policy has been written by the school Computing and PSHE subject leaders and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Planning and Organisation

Online Safety should be focused upon in all areas of the curriculum and staff should reinforce Online Safety messages during computing lessons. The Computing Subject Leaders have a clear, progressive and up-to-date Online Safety education programme as part of the Computing curriculum/Online Safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience.

In the Foundation Stage, pupils are taught to not give out any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At St Mary & St Paul's CE Primary School, we do expect children of this age to be supervised whilst using the internet. Reception pupils take part in the school "Safer Internet Week" using age appropriate CEOP resources.

In Key Stage One, pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and make sure that an adult knows what they are doing online. Teachers model appropriate online behaviour when communicating with others.

There are four key messages taught at Key Stage One:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.
- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

In Key Stage Two, themes taught in Key Stage One are built upon. In addition, pupils are made aware of online experiences which could cause potential danger, e.g. use of social networking, gaming sites and downloading or installing new applications. Links are made between inappropriate sharing of personal information and the dangers this can pose in the real world. Relevant resources from CEOP, Childnet and SWGfL are used during "Internet Safety Week" and other resources can be accessed throughout the year on the school website. In Key Stage Two, children also develop their research skills, especially through use of their iPads. They are taught about plagerism and the need to upload copyright laws.

Resources

Online Safety resources are mainly online safety websites – provided by the ICT / Computing coordinator. Information about new resources/websites are communicated to staff via email.

Inclusion

At St Mary & St Paul's CE Primary we believe that all our children should be given the opportunity to achieve as well as they can in everything they do.

Acceptable Use of Personal Equipment - Children

Use of Facebook / Social networking sites

Children are not permitted to use social networking sites on school premises. Both on computers or mobile devices. Children are also reminded of minimum age guidelines for various social networking sites, as part of their Online Safety lessons.

Use of Mobile Phones

Mobile devices must be switched off and handed to Mrs Evans at the start of each day.

Children are not allowed to take mobile phones on any school residential trip

Mobile phones brought into school are entirely at the staff member/ visitors' own risk. St Mary & St Paul's CE Primary School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Where parents or students need to contact each other during the school day, they should do so only through the school's telephone.

Email

Children may have access to messaging systems on iOs applications such as SeeSaw, though all messages must be approved by the class teacher before the messages go live. Other messaging or e-mail solutions may be used when appropriate for a particular year group.

Cyber-Bullying

Safer Internet Week is held annually with up to date Online Safety guidance. The school website has links to cyber-bullying advice. Incidents of cyber-bullying are dealt with by leadership team and communicated to parents where necessary.

Acceptable Use Policy (AUP)

The AUP is written and distributed to all pupils during the Autumn term of the school year and signed by parents/guardians. The AUP will be reviewed annually.

Acceptable Use of Personal Equipment - Staff

Use of Facebook / Social networking sites

Staff are not permitted to access Facebook or most other social networking sites from a school computer whilst on school premises. Staff are permitted to use Twitter on school computers for educational purposes and networking. Social networking sites can be accessed on a personal handheld device at break times only.

Use of Mobile Phones and other personal mobile devices

See Mobile Phone Policy . Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally- owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Staff will be issued with a school phone where contact with students, parents or carers is required.

If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the designated staff area of the school, e.g. staffroom, an office area.

If any staff member has a family emergency or similar and is required to keep their mobile phone to hand, prior permission must be sought from the a senior manager and the mobile phone should be stored in an agreed location.

Use of Cameras

Images of pupils and/ or staff must only be stored on computers/drivers owned by the school. Images will not be distributed outside the school network (eg. Website/local press/school app) without the permission of the parent/ carer, member of staff or Headteacher.

Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly

available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Photographs published on the website, or elsewhere that include students / pupils will be .selected carefully and will comply with good practice guidance on the use of such image

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website. (see School GDPR Policy and procedures)

Email

Emailing is used as one of the many ways we communicate with each other at St Mary & St Paul's CE Primary School. However, the system should be used responsibly and staff should always act in a professional manner when using the email system. Members of staff should not feel obliged to reply to any emails sent to them in the evenings or at weekends and equally staff should not expect a reply from colleagues outside school hours. Staff are reminded of this at the start of the school year.

Acceptable Use Policy (AUP)

The AUP is written and distributed to all staff during the Autumn term of the school year. The AUP will be reviewed annually.

Incident Management

In this school:

- there is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support will be actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online Safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in Online Safety within the school.
- parents / carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.
- we will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

- any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing Subject Leader, or Leadership Team.
- all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Computing Subject Leader.

Adopted by the Governing Body: Autumn Term ____

Appendices

Acceptable Use Policy

St Mary & St Paul's CE Primary School

Version:	1-0
Approved by:	Governors
Date formally approved:	
Document Author:	
Name of School:	St Mary & St Paul's CE Primary School
Review date:	

Key employee responsibilities

Data Protection

I **must**:

- Follow the data protection principles which state that personal information must be:
  - processed fairly and lawfully;
  - processed for specified and lawful purposes;

    - adequate, relevant and not excessive;
    - accurate, and where necessary kept up to date;
    - not kept longer than is necessary;
    - processed in line with the rights of the information subject;
    - kept safe and secure; and
    - transferred only to countries with adequate security;
- Adhere to any information sharing agreements that are in place for the school.
- Only provide the minimum amount of personal information necessary to respond to any lawful request; and
- Respond to any requests for personal information (Subject Access requests) within 40 calendar days, provided the applicant has put their request in writing and suitable identification has been supplied.

I **must not**:

- Allow unauthorised access to any personal information; and
- Give personal information to anyone internally or externally, unless I am fully satisfied that the enquirer or recipient is fully authorised and legally entitled to the information.

Information security

I **must:**

- Take reasonable measures to protect all School information from unauthorised access, disclosure, modification, destruction or interference;
- Securely manage all information which is personal and/or confidential;
- Return all information and equipment in my possession at the end of my employment with the School;
- Immediately report any information security incident or weakness to a member of the senior management team (Information Asset Owner). If a member of the senior management team is unavailable then I must report it to the headteacher;
- Wear my ID card at all times within School premises and immediately inform my manager and the business manager/adminstration if my ID card is lost or stolen;
- Assume responsibility for all visitors, escort them at all times when they are on School premises, ensure that the visitors log is completed and that visitor passes are obtained and then returned when they leave the premises;
- Ensure that windows are closed and locked when rooms are unattended and at the end of the working day;
- Lock away personal and/or confidential information when it is not required, especially when the room is vacated;
- Collect documents containing personal and/or confidential information immediately from the printer;
- Dispose of information securely and safely when no longer required;
- Dispose of paper which contains personal and/or confidential information by either cross cut shredding or place in a confidential waste bin;
- Dispose of all computers (including PCs, laptops and servers) memory sticks, CDs, and other electronic devices through the office;
- Take reasonable measures to protect paper documents that are taken outside of the school against unauthorised access, misuse or corruption;
- Take care when using electronic messaging, such as email, to transmit any form of information;
- Have appropriate authorisation to take away school assets including information, equipment and software from the school premises;
- Give information stored or processed outside of the school controlled location the same level of protection as it would have if worked on internally;

- Take all necessary precautions to prevent loss, damage or theft of information in my care;
- Ensure that encryption facilities are available and working on any IT equipment used for remote working;
- Ensure sensitive personal and/or confidential information is **only** ever sent by fax where there is no reasonable alternative AND risk to a child and/or the school if the information is not sent by fax. If sending a fax follow these requirements:
    - Confirm that you have the correct fax number for the recipient.
    - Care must be taken when dialling to ensure that the correct number is entered.
    - Before sending personal, sensitive and/or confidential information first confirm the presence of the specific recipient by 'ringing ahead' and asking the recipient to be ready to receive the fax.
    - Cover sheets must be used with all fax transmissions. The cover sheets must not be used to transmit personal, sensitive and/or confidential information, separate sheets must be used.
    - When a fax number is entered manually, the sender must visually check the recipient's fax number against the cover sheet before starting transmission.
    - Once transmission is complete check the fax confirmation sheet to confirm that the receiving fax number and number of sheets are correct. Then telephone the intended recipient to confirm that they have received the fax in full.
    - If the confirmation sheets shows that it is not the correct fax number contact the recipient immediately by telephone if the number is available, or fax if not and ask them to destroy the original fax.
    - Once you have sent and/or received a fax remove it from the fax machine immediately and do not leave it on the top of the machine to invite potential unauthorised access.
- Ensure that I follow these requirements if I am home working:
    - Only take the minimum information home in order to do my work;
    - Ensure that, where possible, I lock away personal or confidential information (for example information which if lost or stolen would cause an individual harm or distress);
    - Ensure that I keep paper documents containing personal or confidential information separate from valuable items, for example remove from laptop bags, handbags, and so on;
    - Ensure that when I leave my home, if council information is stored inside, I will lock all doors and windows and set a burglar alarm if one is fitted;
    - Only take copies of paper files or electronic documents containing personal or confidential information home rather than originals, unless there is no alternative. Dispose of the information in a secure way when no longer required.
    - Must not include identifying personal information on documents used to collect personal information unless absolutely necessary, for example when collecting information on vulnerable people;
    - Must not leave paper or electronic files where they could be viewed by others, including family members;
    - Must not put confidential or personal information in a domestic waste or recycling bin at home;
    - Must not remove a paper file from the school unless absolutely necessary, permission has been given and it can be stored securely at home; and
    - Must not use a personal (non school) e-mail account for school business.

- Change my password if I think that someone else has seen it;
- Use the screen saver lock when working away from the computer (for Windows computers press CTRL+ALT+DEL and click on lock computer) or log out of my session;
- Secure a school laptop when it is left unattended i.e. by using a 'Kensington' (steel cable) lock or by locking it away in a cupboard;
- Store equipment, including laptops, out of sight in a locked cupboard overnight and at weekends if I don't take my laptop with me;
- Be aware of the environment around me and report any risks and/or concerns I have, for instance doors not locking.
- Keep paper files securely at all times;
- Always keep items close to me if using public transport;
- Place laptops out of sight in the boot and lock the boot if travelling by car;
- Not leave equipment and/or documents unattended (especially in vehicles). However, there may be exceptional circumstances where leaving a laptop in the boot of a car could be considered safer than carrying the equipment with you. In these instances you should carefully consider the risks involved as you will be asked to justify your decision, should there be a breach in information security; and

I **must not**

- Ignore or exploit any information weaknesses;
- Transfer my ID card to anyone else;
- Let anyone avoid or bypass security by following me or another person through an access control door, unless you feel it is unsafe to do so. If you do feel unsafe and a person manages to gain access, inform the site manager and the headteacher immediately; and
- Knowingly leave personal information on printing facilities including copiers, printers and faxes.
- Write my passwords down;
- Disclose and/or share my passwords with anyone;
- Use a word or phrase in a password that can easily be guessed – names, sports teams, and so on;

IT acceptable use

I **must**

- Save all data (including word documents and spreadsheets) to the appropriate fileserver;
- Only use encrypted portable storage devices (including laptops);
- Ensure that any electronic data authorised to be shared with a third party is undertaken in a secure manner approved by the school;
- Arrange all movements and redeployment of IT equipment through the school office;
- Notify my line manager, the headteacher and the school office if any IT equipment is lost or stolen;
- Return IT equipment to my line manager or the school ofice immediately upon request;
- Report any suspicious messages and/or files to the Councils IT Service Desk,
- Report any virus warnings to the Councils IT Service Desk,
- Use officially provided email addresses to send all business related emails. Officially provided email addresses include "@knowsley.gov.uk" and "@*.klear.org.uk";
- Use encrypted email solutions (e.g. Egress Switch) when sending emails that contain sensitive personal and/or confidential information outside of the Council's secure email service;

- Use the school email system for school related matters only and not for personal use
- Comply with the Data Protection Act for any data being transferred, especially when transfer is outside of the European Economic Area (EEA);
- Ensure that all recipients of an email are entitled/authorised to view the contents;
- Seek advice from my line manager, senior management team, the HR Service or the Councils IT Service if I have any queries about business use of email
- Undertake personal use of email in my own time, ensure that such use is lawful and complies with the school's other policies and ensure that personal use of does not have a negative impact on the School or its partners; and

I **must not:**

- Store personal and/or sensitive personal data on unencrypted portable / removable storage devices (inc. laptops, USB drives etc.);
- Allow third parties to access any school information without confirming with my manager that they are authorised to have such access;
- Attempt to change any administration settings on computers that I use;
- Transmit by any electronic means any message, file or attachments which I know or suspect to be infected with a virus;
- Download any software (including screensavers) without the prior written approval of the Headteacher;
- Forward virus warnings;
- Send or forward business emails or electronic files which contain personal and/or sensitive personal information to my home email address;
- Send emails to people if I am unsure if they are entitled/authorised to see the content;
- Use school email facilities for the transmission of unsolicited commercial or advertising material, chain mail or other junk-mail of any kind to colleagues or any other organisation;
- Create or transmit anonymous messages, i.e. without clear identification of the sender;
- Create or transmit material which could bring the school or its partners into disrepute;
- Send emails to large distribution groups without the authorisation of my manager;
- Send emails with large attachments without a legitimate business reason (5Mb is classed as large);
- Allow personal email use to interfere with performance or priorities of my or another person's duties;
- Conduct any form of private or third party business using the school's email service;
- Send excessive emails or large attachments; and
- Use business email addresses to register for personal websites (for example banks and online shopping), personal use of social networking sites or to confirm orders for personal goods or services.
- Use any other email address other than the school address provided to transfer data concerning children or families.
- Use the internet in school inappropriately