South Baddesley CE Primary School

Acceptable use of IT Policy 2023-24

Purpose of Policy :

At South Baddesley CE Primary School we recognise the valuable contribution that IT can have to the development of effective and innovative learning for all. In order for IT to be used appropriately, we have developed clear expectations and guidance for all members of the school community.

This policy must be read in conjunction with:

- Freedom of Information Legislation and GDPR regulations
- Legal Framework for illegal use of the Internet,
- Acceptable use of Social Media Policy
- Email, Internet and Intranet Monitoring Policy
- Guidance documents for staff – Dos and Don'ts
- Disciplinary procedures found in the Performance Management Policy
- School Safeguarding procedures in-line with *Keeping Children Safe in Education 2023*
- SBS Online Safety Policy
- SBS Photography and Filming Policy

This policy provides advice to staff in relation to potential risks and consequences in relation to the inappropriate use of their own personal use of IT, where it is inconsistent to the expectations of staff working with children and young people.

We provide staff with sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. At South Baddesley we have sought advice from external professionals, including trade unions as well as developed our use of resources from agencies such as Childnet (www.childnet.com).

Roles and Responsibilities

This policy applies to all teaching and support staff, trainees, volunteers, the school governing body, external providers including sports coaches, music teachers, catering staff and contractors who are providing services on behalf of the school or Hampshire County Council. In this policy these individuals are collectively referred to as staff or staff members.

Head teacher and Governors	Monitor the effective application of the *Acceptable Use of IT Policy*. Ensure that the policy is reviewed at least annually and updates are communicated to all staff. Ensure that appropriate training is provided for all staff. Complete regular checks on the filtering systems using this website: http://testfiltering.com/ Complete Cyber Security training and update all staff.
Senior Leaders	Support the HT in the successful implementation of the policy within the school. Plan for the effective teaching and learning of Internet Safety for all pupils. Ensure children are aware of the benefits and risks of internet use. Provide guidance and support for staff on the teaching and learning of Computing. Review the impact of the PoS on pupil's learning of computing skills, attitude and understanding.
IT Technician -External	Provide technical support for staff. Ensure that appropriate filters and blocks* are applied on the network and to work with the HT if filters are breached that any unacceptable use of IT is reported immediately to the HT and/or IT help desk. Agree the downloads of Apps and ensure that this task is completed safely and in-line with the Acceptable use of IT Policy. *Blocks are in place for all recommended sites as well as additional sites requested by the HT.
Class teachers	Follow PoS part of the Lighthouse and Explorer Curriculum. Ensure that pupils are provided with high-quality Internet Safety lessons. Ensure all access to the internet is supervised and pupils feel safe when using the internet. Any unacceptable use is reported to the HT or senior leadership team.
All staff	Consult with the IT Technician prior to making any downloads. Portable storage devices are not used at South Baddesley. All documents and records are recorded on the schools systems of Google Drive, Arbor and My Concern.
Pupils	Sign and agree to follow pupils' Online Safety contract in school Online Safety Policy
Parents , carers, external providers, volunteers and contractors	To follow the school policy of Online Safety Policy when in school. Support school in the successful implementation of policy through good communication with school. Where possible, sign up to the national Online Safety resources.

Resources

This policy applies to all IT resources and equipment within the school and resources that have been made available to staff for working at home. IT resources and equipment includes:

- computer resources,
- use of school internet access and email systems,
- software (including Arbor and My Concern),
- school telephone systems,
- cameras and recording equipment,
- intranet and virtual learning environment,
- and any other electronic equipment used in the course of the employee or volunteer work.

Access

School staff will be provided with a login where they are entitled to use the school IT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of school hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system, Arbor, DFfE Access and Reporting) will be restricted to nominated staff or specific permissions and access will be agreed.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed. This is in-line with the SBS Photography and Filming Policy.

If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used

in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

Provision of the Internet in school:

SBS provides Internet connection through the Harrap Service Provider. The school is connected through HPSN2, a high quality and fibre-optic network.

There is a high-quality content filter applied to ensure, where possible, inappropriate content is filtered. Whilst this is normally a robust system, inappropriate content may occasionally get past the filter. In the case of this happening, staff and pupils follow guidance set out in the IT Contract.

The use of mobile devices to access the Internet is not currently possible due to limitations of the school site. This provision will continue to be monitored.

Communication with parents, pupils , governors and external agencies

The school communicates with parents and governors through a variety of mechanisms. The points below indicate who is normally authorised to use these different methods of communication and how this will be managed in school.

Communication method:	**Who and how?**
School telephones	The following people are routinely able to access the school telephone system to communicate with parents and external agencies regarding pupil welfare or learning. ● HT and Senior Leadership Team ● Class teachers ● Admin staff

	• Pastoral staff • Medical Lead Co-ordinator It is best-practise for all other staff to discuss with HT or Senior Leadership Team before using the school telephones to discuss a pupil.
Letters	Most letters are sent home electronically and are sent via Arbor so that a record is kept. All letters should be sent home on headed paper or paper with the school logos on. When a letter is relating to an off-site visit, permission from the HT must be sought following the procedure for planning off-site visits.
Email	School email accounts are provided for all staff, including: • HT and senior leadership team • Class teachers • Admin staff • Pastoral staff • Site staff • Medical Needs Co-ordinator • Sports Event Lead Email must not be used to communicate with parents, unless this has been arranged with the HT. Email correspondence may be used within normal working hours to communicate with governors, external agencies and professionals and colleagues. All staff should use the SBS out of office message on school email accounts. *SBS automated email response:* *Thank you for getting in contact. Whilst we monitor emails regularly and encourage efficient communication, it may take up to 5 working days to respond to this message.* *If this email is urgent, please call school during working hours.*
Home-Visits	When home-visits take place, staff must always work in pairs. Prior arrangements will be made with HT in preparation for all home-visits and in-;ine with updated school risk assessments.

Communications with pupils

Under normal circumstances, staff must not be using any of the above communication methods to communicate with pupils. If a member of staff needs to contact a pupil via any of the above methods, this must be approved by the Headteacher.

Electronic communication with pupils is via Google Classroom.

Published content on the school website

Contact information published on the school website includes the school email address and telephone number.

Permission to publish images of children on the school website is gained from parents. Pupil's full names will not be published on the school website, particularly in association with any photographs.

The Headteacher takes overall responsibility for ensuring the content on the school website is accurate and appropriate. School governors are responsible for providing regular reviews of the school website.

Social Media

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

Unacceptable Use

Appendix 3 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of IT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;

- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;

- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;

- to communicate anything via IT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;

- to communicate anything via IT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils;

- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

- to collect or store personal information about others without direct reference to The Data Protection Act;

- use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

- to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school;

- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people;

- Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about

the use of IT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or IT lead if applicable.

- Where an individual accidentally or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

- Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

Personal and Private Use

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

- interfering with the individual's work

- relating to a personal business interest

- involving the use of newsgroups, chat lines or similar social networking services

- at a cost to the school

- detrimental to the education or welfare of pupils at the school

Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other IT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

Security and Confidentiality

Any concerns about the security of the IT system should be raised with a member of the senior leadership team.

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

Staff should use SBS Google Drive to store all work relating to the pupils of SBS. Staff may only use memory sticks to store subject content that is not related to any pupils at SBS.

Any document that includes high-risk data will be saved on

- SBS Google Drive
- My Concern - child protection
- Arbor - contact information, enrolment and demographics, behaviour, SEND, including pastoral, meeting and telephone conversation notes.

School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's IT lead.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil IT system and/or VLE.

Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the school's IT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of IT facilities.

Monitoring

The school uses Harrap's IT services and therefore is required to comply with their email, internet and intranet policies. Monthly monitoring reports are shared with the Headteacher and Deputy Headteacher. The Headteacher also completes termly checks of filtering systems, or more frequently if required.

The school reserves the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised

- to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems

- to gain access to communications where necessary where a user is absent from work

- Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

- To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

Whistle Blowing and Cyberbullying

Staff who have concerns about any abuse or inappropriate use of IT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

It is recognised that increased use of IT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

For further information regarding Whistle blowing please refer to the SBS Whistle Blowing Policy.

Signature

It will be normal practice for staff to read and sign a declaration as outlined in Appendix 4, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to IT facilities. Staff should be aware that in certain instances, inappropriate use of IT may become a matter for police or social care investigations.

Appendix One – Pupil's IT Contract (available on Google Classroom)

Appendix Three – Dos and Don'ts

Appendix Four – Code of Conduct

Appendix Three: Dos and Don'ts

Do's and Don'ts: Advice for Staff

Whilst the wide range of IT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use IT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of IT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- ensure that you do not breach any restrITions that there may be on your use of school resources, systems or resources

- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school's IT resources and facilities
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in IT
- ensure that your use of IT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through IT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pITures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils

Staff Code of Conduct for IT Appendix 4

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of IT for further information and clarification.

- I appreciate that IT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it may be a criminal offence to use the school IT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school IT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of IT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of IT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.

- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based IT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's IT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's IT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……..….

NAME (PRINT): ……