"Achieving The Best For All"

Acceptable use of ICT

Equality at Merdon Junior School Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school. (See Initial Equality Impact Assessment)

Name of Headteacher:	**Thomas Johnston**
Date Policy approved and adopted:	**December 2025**
Date Due for review:	**December 2027**

Acceptable Use of ICT Policy

1.0 Introduction

This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.
This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

2.0 Access

All staffs will be provided with a log on where they are entitled to use the schools ICT 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 Hampshire schools 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 schools 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, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their 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 provide digital cameras and other recording equipment for educational and school business use and it is used away from the 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 policy in relation to use of pictures, is followed and the GDPR regulations and policy is followed.

The school does not provide work 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 schools rather than a direct call from the individual's personal mobile. Schools staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

No mobile telephones or similar hand held devices should be used whilst driving on school business. Hands free devices can be used but at the drivers own risk and not recommended by the schools.

School phone system may be used by staff for private calls in an emergency.

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

3.0 Communication with parents, pupils and governors

The school communicate with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. The school must indicate to staff if any other staff are permitted to make contact using the systems below:

School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

Text System – Senior Leaders and Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

Letters – Normally all teachers may send letters home, but they are required to have these approved by the Headteacher before sending.

Email – school email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email. All governors are required to have a specific governor email for all communication.

Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the risk assessment on home visits.

Staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

4.0 Social Media

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 Social Media Policy which contains detailed advice on the expectations of staff when using social media.

5.0 Unacceptable Use

Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. The schools systems and resources must not be used under any circumstances for the following purposes:

to communicate any information that is confidential 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 ICT 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 ICT 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 which does not comply with GDPR regulations

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

6.3 Where an individual accidently 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. The school uses appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where 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.

6.0 Personal and private use

All 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 news groups, chat lines or similar social networking services
- at a cost to the schools
- detrimental to the education or welfare of pupils at the schools

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 ICT 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 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.

7.0 Security and confidentiality

Any concerns about the security of the ICT 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 must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with an encrypted memory pen for such activity, to both protect the integrity of the server and to save space, this should always be used. 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 IT systems. Where problems are encountered in downloading material, this should be reported to the Senior Leadership Team.

Where staff are permitted to work on material at home and bring it in to upload to the school server through their encrypted memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Staff who are given authorisation will be provided with crypto cards to access the school systems at home.

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

Whilst any members of staff may be involved in drafting material for the schools website, only authorised users will be permitted to upload material to the website.

The Finance Officer is 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 ICT facilities does not compromise rights of any individuals under the Data Protection Act (GDPR). This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through encrypted memory pens or through crypto cards. 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 ICT facilities.

8.0 Monitoring

The school use Hampshire County Council's ICT services and therefore are required to comply with their email, internet and intranet policies.

The school and County Council reserve 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 and 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.

9.0 Whistleblowing and cyberbullying

Staff who have concerns about any abuse or inappropriate use of ICT 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.

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of 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.

10.0 Compliance

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 ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

Do's and Don'ts: Advice for Staff **Appendix 1**

Whilst the wide range of ICT systems and resources available to staff have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT 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 ICT 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 restrictions 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 ICT resources and facilities

be aware that the IT systems will be monitored and recorded to ensure policy compliance

ensure you comply with the requirements of the Data Protection Act/GDPR when using personal data

ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely following GDPR policy

report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to EHT

be aware that a breach of your 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 your use of ICT 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 ICT 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 systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use 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 EHT or Head of School if you receive inappropriate content via email
- be aware that the school email systems 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 is believed that there is inappropriate use
- seek support to block spam
- alert your EHT 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

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

Use of telephones, mobile telephones and instant messaging

Don't

- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line
- upload any material onto the school website that doesn't meet style requirements and without approval

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

Don't

- send messages that could be misinterpreted or misunderstood

- use personal or school mobile telephones that are not hands free when driving

- inappropriately access, view, share or use

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 policy
- ensure that parental consent has been given before you take pictures of pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, intranet without prior agreement from a member of senior leadership team.

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

Don't

- spend 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

Evaluation and Review

Date of Ratification	December 2025
Date for Next Review	December 2027
Comments:	