Hook-with-Warsash Church of England Academy

IT Policy

Appendix 3 of the Safeguarding Policy

Signed:

Chair of Governors _____

Headteacher_____

Reviewed: June 2026

Date to be reviewed: October 2027

"Let Your Light Shine"

To provide an inspirational environment based on Christian values where individuals can excel and flourish academically, socially and emotionally, preparing them for life's journey.

Hook with Warsash
The Acceptable Use of ICT Policy

1.0 Introduction

1.1 This policy has been developed on behalf of all the staff and headteacher at the Academy and has been ratified by the Governing Body.

1.2 This Policy should be read in conjunction with other relevant Academy and County Council policies, procedures and Codes of Conduct including: Safeguarding Policy, Disciplinary Procedure, and Computing and Online Safety Policy.

1.3 Schools are encouraged to ensure that staff are given 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. Schools and their staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com). Advice can also be sought from professional associations and trade unions.

2.0 Application

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

2.2 The policy applies in respect of all ICT resources and equipment within the Academy and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of Academy internet access and email systems, software (including use of software such as SAP and SIMS), Academy 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.

2.2 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.

3.0 Access

3.1 School staff will be provided with a log on where they are entitled to use the school 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.

3.2 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 Academy business outside of normal office hours.

3.3 Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), SIMS, RAISE Online, FFT) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their Academy 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.

3.5 Where the Academy provides digital cameras and other recording equipment for educational and Academy business use and it is used away from the Academy 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 Academy's policy in relation to use of pictures, is followed.

3.6 If the Academy does not provide Academy 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 Academy 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 Academy rather than a direct call from the individual's personal mobile. Academy staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

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

3.8 Whether Academy staff have access to the Academy telephone system for personal use will be confirmed by the Academy. Where such use is made of this facility, it

must be done during break periods, must not be excessive and the Academy should require either the cost of the call or a donation to be made towards the cost of the call.

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

4.0 Communication with parents, pupils and governors

4.1 The Academy communicates 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. Academy must indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 Academy 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.

4.1.2 Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the Academy's policy on home visits.

4.2 Under normal circumstances, Academy 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.

4.3 Where pupils are submitting work electronically to Academy staff, this must be undertaken using Academy systems and not via personal email unless otherwise agreed.

5.0 Social Media

5.1 Academy 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 Academy can lead to disciplinary action, including dismissal.

5.2 **Friends/Befriending:**

One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. The Academy prohibits staff from accepting invitations to "friend" pupils, or pupil's family members/friends.

5.2.1 Staff must not initiate friendships with pupils, or pupils' family members/friends, under any circumstances. The only exception to this is in the case or pre-existing personal relations with parents and/or where staff are also parents of pupils at the Academy. It is never permissible however to have any contact whatsoever with pupils of the Academy through social networks. Where communications are made with parents, staff are required to adhere to the requirements below relating to content of interactions.

5.2.2. Staff who maintain social networking friendships with work colleagues, are required to adhere to the requirements below relating to content of interactions.

5.2.3 Staff must not make reference on social networking sites to the Academy, its employees, pupils, and their families. If staff adhere to this recommendation then the personal content of an individual's social networking memberships is unlikely to be of concern to the Academy. If employment at the Academy is referred to, then the information posted would need to comply with the conditions set out below.

5.2.4 Any references made to the Academy, its employees, pupils and their families, should comply with the Academy's policies on conduct/misconduct, equal opportunities, and bullying and harassment.

5.2.5 Staff must not post information on a social networking site which is confidential to the Academy, its employees, its pupils or their families.

5.2.6 Staff must not post entries onto social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the Academy into disrepute.

5.2.7 Staff should not use the Academy logo on their own personal social networking accounts, and should not post any photographic images that include pupils or members of staff.

5.2.8 Staff must not download copyrighted or confidential information.

5.2.9 Staff must not express personal views which could be misinterpreted as those of the Academy.

5.2.10 When posting any information onto a social networking site, staff must not post any entry that puts their effectiveness to perform their normal duties at risk.

5.2.11 If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the Academy, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with their head teacher/line manager in the first instance. Guidance is also available from HR/Payroll and trade unions.

6.0 Unacceptable Use

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

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

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

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

6.1.4 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;

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

6.1.6 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;

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

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

6.1.9 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 Academy;

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

6.2 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 or Computing Co-ordinator 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. 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 Academy staff are using Academy 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.

6.4 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.

7.0 Personal and private use

7.1 All Academy 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:

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

7.1.2 interfering with the individual's work

7.1.3 relating to a personal business interest

7.1.4 involving the use of news groups, chat lines or similar social networking services

7.1.5 at a cost to the Academy

7.1.6 detrimental to the education or welfare of pupils at the Academy

7.2 Excessive personal use of Academy 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 Academy will seek reimbursement from the member of staff.

7.3 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.

7.4 Where Academy staff have brought their own personal equipment such as mobile telephones, laptops and cameras, into the Academy, 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 Academy data/images are deleted following use of the equipment.

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

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with the Data Protection Officer (DPO) a member of the Senior Leadership Team.

8.2 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.

8.3 Academy staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the Academy server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should 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 Academy's systems. Where problems are encountered in downloading material, this should be reported to the Academy's Computing Co-ordinator.

8.4 When staff are working on material at home they must use the Academy issued devises where practical. When not practical they can bring it in to upload to the Academy server through their memory pens and they must ensure that they have undertaken appropriate virus checking on their systems.

8.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the Pupil Area.

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

8.7 The Academy 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 Academy based and Academy issued equipment.

Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

8.8 Staff must ensure that their use of the Academy's ICT 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.

8.9 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.

8.10 All staff/governors must undertake annual e-safety and cyber security training as specified by the Academy.

9.0 Monitoring

9.1 The Academy 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:

9.2 to ensure that the security of the Academy's hardware, software, networks and systems are not compromised

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

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

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

9.4 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.

10.0 Protection from Computer Viruses and Ransomware

10.1 Preventative Measures

- All school devices are protected by up-to-date antivirus and anti-malware software, managed by our IT support provider.

- Two factor authentication is used where possible.
- Regular system scans are scheduled, and software updates are installed promptly.
- Staff and pupils are trained to recognise suspicious emails, attachments, and links.
- Only authorised software is installed on school devices. Staff and pupils must not download or install software without permission from IT support.
- Removable media (e.g. USB drives) are virus checked by the staff before they use them.

10.2 Response and Recovery

- Any suspected virus or ransomware incident must be reported immediately to the Data Protection Officer.
- Devices suspected of infection are isolated from the network until cleared.
- Regular backups of important data are maintained and tested for integrity.
- In the event of a ransomware attack, the school will follow DfE and local authority guidance, and will not pay ransoms.

10.3 Staff and Pupil Responsibilities

- Staff and pupils must not attempt to bypass security controls.
- Emails from unknown senders should be treated with caution and reported to the DPO if suspicious.
- Passwords are kept confidential, strong, and changed regularly.

11.0 Whistleblowing and cyberbullying

11.1 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. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

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

11.3 Further advice on cyberbullying and harassment can be found in the Safeguarding Policy and in Cyber bullying: Practical Advice for Academy Staff.

12.0 Signature

12.1 It will be normal practice for staff and governors to read and sign the declaration in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

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

In all use of ICT, the Academy's practice conforms with the requirements of the General data Protection Regulations 2018

Reviewed by Committee: October 2026
Date for Review: October 2027

Pupil Discipline, Curriculum & Early Years Committee

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

Whilst the wide range of ICT systems and resources available to staff, both in Academy and outside of Academy, 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 Academy.

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 Academy 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 Academy's ICT resources and facilities*
- *be aware that the Academy'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 Academy 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 Academy'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 Academy'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 ICT
- 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 Academy systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use Academy 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, and Academy intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the Academy'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 Academy 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 Academy 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 Academy or HCC intranet
- upload any material onto the Academy 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 Academy's policy on use of personal mobile telephones
- ensure that you reimburse your Academy for personal telephone calls as required
- use Academy 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 Academy mobile telephones to take images of colleagues, pupils or of the Academy without consent or approval.

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

Don't

- bring personal recording equipment into Academy 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

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 Academy procedures for contacting parents and/or pupils
- only contact pupils and/or parents via Academy 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

IT security

Dos

- **Do use strong passwords**
  Create passwords with a mix of letters, numbers and symbols. Change them regularly and never share them.
- **Do lock your screen**
  Always lock your computer (Windows: Win + L, Mac: Ctrl + Cmd + Q) when you leave your desk, even briefly.
- **Do check email senders**
  Look carefully at sender addresses, especially if asked to click a link or download an attachment.
- **Do report suspicious emails**
  If you receive a suspicious message, don't click on anything – report it to the Data Protection Officer.
- **Do keep software updated**
  Allow updates to install on your computer and devices as prompted.
- **Do save work to the school's secure network**
  Use approved cloud storage or the school server – not personal USB drives or unapproved services.
- **Do use 'Bcc' for group emails to parents**
  Protect privacy by using blind carbon copy when emailing groups.
- **Do follow the Acceptable Use Policy (AUP)**
  Make sure you understand and comply with the school's IT policies.
- **Do attend IT security training**
  Take part in any staff briefings or online courses provided.

Don'ts

- **Don't share your login details**
  Never give your username or password to anyone, even colleagues.
- **Don't open unexpected attachments or links**
  If you aren't sure about an email or its contents, don't open anything – check first.
- **Don't install unauthorised software**
  Only install programs approved by IT support.
- **Don't use personal email for school business**
  Always use your school email account for work-related communication.
- **Don't leave devices unattended and unlocked**
  Always lock your computer or tablet if you step away.
- **Don't use unapproved cloud or file sharing services**
  Stick to the platforms approved by the school for storing and sharing files.
- **Don't ignore software update prompts**
  Updates patch security holes – install them as soon as you can.
- **Don't plug in unknown USB drives**
  If you find a USB stick or are given one from outside school, ask IT to check it first.
- **Don't bypass security settings**
  Don't attempt to turn off firewalls, antivirus or other security measures.

Staff and Governor Code of Conduct for ICT Appendix 2

To ensure that members of staff and governors 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 Academy's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT 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 ICT use may also include personal ICT devices when used for Academy business.
- I understand that it may be a criminal offence to use the Academy ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the Academy or which I do not have the authority to share.
- I understand that Academy information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of Academy 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 Academy ICT 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 ICT.
- 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 Academy'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 Academy, taken off the Academy 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 ICT 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 Academy, 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 Academy'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 online-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-Academy based ICT facilities can have implications for my employment at the Academy where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The Academy may exercise its right to monitor the use of the Academy's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the Academy's ICT 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): ……