Acceptable Use of IT & E-Safety

Policy & Procedure

If printed this is an uncontrolled document – refer to CLS Website for the latest version

Reviewed **February 2021**
Next Review **February 2024**

Table of Contents

PERSONAL USE OF ICT 5

PRIVACY WHEN USING ICT 6

CONFIDENTIALITY WHEN USING ICT 6

MISUSE AND MONITORING 7

MONITORING OF ICT SYSTEMS 8

USING COMPUTER SYSTEMS 10

SECURITY OF COMPUTER SYSTEMS 11

REMOVABLE MEDIA 12

EMAIL USE 13

EMAIL ETIQUETTE 15

INTERNET USE 16

SUPPLEMENTARY INFORMATION: SUMMARY OF ACCEPTABLE USE OF ICT 17

IT SECURITY 19

EMAIL & INTERNET 19

E-SAFETY - AN OVERVIEW 20

Acceptable Use of IT Policy

Document Title	**Acceptable Use of IT Policy**
Reference Number	**IT-001**
Version Number	**V1.1**
Date of Issue	**15/02/2018**
Latest Revision	**29/1/2021**
Distribution	**All employees**
Owner	**IT Manager**
Policy Lead(s)	**IT Manager/Business Manager/Principal**
Department	**Information and Communication Technology**

Scope

This policy explains the steps needed to be followed by both managers and employees of Church Lawton School in order to ensure the School applies best practice and complies with legislation.

Responsibility for reviewing this policy lies with the IT Department, in conjunction with the Business Manager and School Principal. This policy is subject to review on an annual basis or sooner if necessary to ensure that practices properly reflect the policy, and that the policy is feasible and effective.

Policy Summary

The purpose of this policy is to set out standard working practices for the use of Information and Communication Technology (ICT) within the School. This includes the computing, email, Internet, telephone and fax facilities provided for staff by The National Autistic Society Academies Trust Church Lawton School (NASAT CLS).

The NASAT CLS' computing and telecommunications systems have become vital business tools and the School recognises that access to these facilities increases staff effectiveness and productivity. Furthermore, the introduction of these electronic systems has contributed to improving communication between staff and external contacts. However, their use also poses potential security risks and can be counter-productive if used without policy guidelines.

The School has made a significant investment in information technology and electronic communication systems. Access to computing, email, Internet and telephone facilities is provided for use by employees for the benefit of the business. These systems and any documentation or correspondence produced using these systems, are the property of the School. The NASAT CLS seeks to create an appropriate balance between the protection of the employee - under the UK statutes governing human rights, personal privacy and data privacy - and the right of the School under UK statute, to limit the use of its computer and telecommunications systems, and its right to monitor the uses of these systems.

All users are responsible for ensuring that these School facilities are used in a professional, ethical and lawful manner. In addition to this, the policies detailed below govern use of the School's computing and telecommunications systems. These policies form part of your terms and conditions of employment. Infringement may give rise to appropriate disciplinary action, which can include dismissal.

It is of critical importance that you understand and comply with these policies. If there is anything you do not understand, it is your responsibility to seek further clarification from your line manager.

Personal Use of ICT

The School's computing and telecommunications systems are primarily for business use. Occasional and reasonable personal use of email, Internet access and the telephone/fax network is permitted at your manager's discretion, provided that it:

- does not interfere with the performance of your duties,
- does not interfere with the operation of the Schools' business or systems,
- takes place substantially out of normal working hours (e.g. at lunchtime),
- does not commit the Society to anything other than marginal costs,
- does not involve personal commercial activity (e.g. offering services or merchandise for sale),
- Otherwise complies with this policy.

Privacy when using ICT

Whilst personal use of the systems is permitted, you should nevertheless have no expectation of privacy in respect of personal use of any of the School's computing and telecommunications systems. However, the School will only open files or emails that are clearly personal where it is necessary to do so for business purposes.

Remember that damaging or confidential files, email, Internet use information or telephone logs may have to be disclosed in litigation or in investigations by other authorities. You should be aware that deleting a file or email may not eliminate it from the system and consequently the School, or a third party with good reason, may still access it.

Confidentiality when using ICT

It is very important for you to understand that electronic and telecommunications systems are neither confidential nor secure and all of our systems are potentially accessible by third parties other than the intended recipient. This together with the restrictions imposed by the General Data Protection Regulation 2018, means that you must never reveal confidential information about anyone, without explicit permission from the "owner" of that confidential information.

This includes, but is not limited to, confidential information about pupils, parents, staff, contractors, and competitors. Thus, even though it may be simpler to transmit confidential information using email, the Internet or telephone, do not be tempted to do so. The School may take disciplinary and/or legal action against you for inappropriate disclosure of confidential information regarding or belonging to the Society, or to an individual or company dealing with the Society. Legal action may also be taken after the termination of your employment.

Please refer to the separate NASAT and NAS Data Protection Policy Documents for further information on dealing with personal data.

Misuse and Monitoring

The School has a duty to protect its staff from harassment and from having to work in a hostile environment. Its staff similarly have a duty not to harass, deliberately or by default, including by use of the computing, email, Internet and telephone systems. You should be aware that whether any remark is harassing, discriminatory or offensive will depend on how it is received by the recipient as well as by those around you, regardless of your intention as the originator. You need to be particularly careful about the perceptions of others differing from yours; what you see as funny or clever may be received with horror and an allegation of harassment. Harassment may be a criminal offence; it is definitely a serious employment offence and will be dealt with accordingly. As stated earlier, all users are responsible for ensuring that the School's computing, email, Internet and telephone/fax facilities are used in a professional and ethical manner that is consistent with this policy. Furthermore, all users of the School's systems must not be engaged in the:

- Deliberate violation of any laws and regulations;
- Deliberate origination or distribution of chain letters or other "junk" email;
- Deliberate storage, use, downloading or distribution of pirated software or data;
- Deliberate introduction and/or passing on of any virus, worm, Trojan horse, or other malicious code;
- Disabling or overloading any computer system or network, or circumvention of any system intended to protect the privacy or security of another user;
- Uploading or distribution of any software licensed to the School, or data owned or incensed by the School;
- Deliberate viewing, storage, downloading or distribution of pornographic or sexually explicit or otherwise offensive material.

Never email, view or otherwise communicate any illegal, racist, sexist, defamatory, obscene, pornographic or otherwise abusive or threatening messages or images. You must not send or forward jokes or other material which refer to race, sex or disability, even if they seem harmless to you.

Sending sexual innuendoes or pestering messages may lead to an allegation of sexual harassment.

Similarly, any communications which refer to an individual's race or colour may result in liability for race discrimination. Misuse of these sorts could result in liability not only for you but also the School as anything done by any staff member in the course of employment is also treated as having been done by the employer.

Violation of any of the above at any time will be treated as a disciplinary matter and may be seen as gross misconduct, meriting summary dismissal.

Monitoring of ICT Systems

When using the School's computing and telecommunications facilities, employees should be aware that the Society may monitor communications, regardless of whether the use is for business or personal reasons. All use of the School's facilities including personal, may be inspected, examined, reviewed, audited, disclosed or monitored by the School without notice when there is a clear business purpose, to ensure that the system is not being abused and to protect the School from potential damage or disrepute.

Types of communications to which this may apply include incoming and outgoing telephone calls, emails as well as records of interaction with websites. The School has software and systems in place that can monitor and record all computing and telecommunications facilities usage.

You should be aware that our security systems are capable of recording (for each and every user) each web site visited, and each file transferred into and out of our internal networks. The School also has access to detailed telephone call records. We reserve the right to carry out monitoring activities at any time when we believe it is necessary for business purposes, both inside and outside office hours. Routine monitoring is most likely to be in the form of audits and/or spot checks. However, the School will only monitor individual employee communications where this is permitted by law and is necessary or justifiable for business reasons. Reasons for monitoring are based on statutory provision and include:

- To establish existence of facts (e.g. to provide evidence of commercial transactions in cases of dispute);
- To ascertain compliance with regulatory practices and procedures (e.g. to ensure that employees are not in breach of any policies or procedures);
- To ensure secure and effective operations (e.g. protecting systems against viruses or hackers);
- To ensure employees are achieving the standards required (e.g. monitoring for quality control and for staff training purposes);
- To determine whether the purpose of an email is relevant to the business (e.g. checking an employee's email during his or her absence);
- To detect unauthorised or criminal use (e.g. to conduct investigations into suspected fraud).

Monitoring may involve gathering specific information as set out in the examples below. Where there are reasonable grounds to believe that misuse has taken place or there has been a breach of the law/School's codes of conduct, the School may conduct a more detailed investigation, potentially involving further monitoring and review of stored (but employee-deleted) data held on a server/disk/drive or other historical/archived material.

Employees are reminded that deleting a file or email may not eliminate it from the system and consequently the School or a third party with good reason, may still access it.

Gathering specific information may involve examining and/or monitoring:

- The number and frequency of emails to and/or from a particular mail box;
- Incoming/outgoing calls;
- Telephone conversations;
- Emails sent from and received into a particular mailbox and/or stored on the server;
- files stores on the server;
- The amount of time spent by a member of staff on the Internet;
- Internet sites visited, and information downloaded.

In short, the nature of the facilities monitoring is not designed to extract evidence of misuse. However, where evidence of misuse becomes known as a consequence of monitoring, it will be investigated thoroughly, and appropriate action taken under existing procedures. The School will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives of an individual's activities.

Using Computer Systems

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of the School's internal computer systems. These policies are in addition to those already set out in sections that apply across the entire range of the School's computing and telecommunications facilities.

To prevent damage to School systems, all computing equipment must be authorised by the IT Department before being used with existing systems. This includes but is not limited to, desktop PCs, laptops, mobile phones, tablets, PDA's and printers. To prevent copyright infringements, security breaches, virus infections and other damage to School systems, all software must be authorised by the IT Department before being installed or used with School systems.

This includes but is not limited to, store-bought and downloaded programs, screen savers, logos, games, video and music files. To make best use of IT resources, staff should regularly review the contents of their files and mailboxes. Unwanted files and emails should be deleted.

IT equipment is expensive and fragile. Staff must ensure they take all reasonable precautions to protect it from damage and theft. Notify the IT department of any IT related problems as soon as you can. This includes information regarding staff that are starting or leaving, as well as any temporary workers that require access to the IT systems.

Applications, websites, systems, and Databases that require sign up or agreement of terms and conditions must not be used without prior authority from the IT Manager, Data Protection Officer and school SLT. Personal details are protected under GDPR, staff must not allow student details to be input into third party systems without authority.

Security of Computer Systems

User IDs and passwords help maintain individual accountability for computing system resource usage. Any staff member who obtains a password or ID must keep that password confidential. Do not write your password down and do not disclose it to anyone. If you think someone else knows your password you should change it immediately. If you need to give a colleague access to your work, it can be done without disclosing your password. Contact the IT Helpline for advice.

To prevent ongoing security breaches network users are required to change their passwords at least every 30 days. You can change your password by pressing **CTRL-ALT-DEL** and clicking on the Change Password button. Network passwords must adhere to the following rules:

- You have to logon to the network to change your password
- You must change your password the first time you logon to a new account
- You must use your new password for at least one day before being allowed to change it again
- Your password has to be at least 6 characters long
- You can't re-use an old password until 5 different passwords have been used
- If you get the password wrong 5 times your account will be locked out for 30 minutes
- Passwords must **not** contain your user name or any part of your full name

IT staff, and anyone with high-level administrative access, are required to have “strong” passwords. In addition to the above principles, strong passwords must adhere to the following:

- Passwords must contain at least one letter AND one numeral AND one non-alphanumeric (e.g. punctuation symbols, but not * or ?)
- Passwords must not be dictionary words (even foreign words) or proper names (e.g. place names)
- Passwords must not be obvious, or words that contain personal information (e.g. your partner's name)

To prevent accidental disclosure of information your workstation will lock automatically after a set period, however you should always lock your workstation when you are away from it. You can lock your workstation by pressing **CTRL-ALT-DEL followed by ENTER**. You can unlock your workstation by pressing CTRL-ALT-DEL and entering your password.

Removable Media

The school seeks to minimise the loss, unauthorised disclosure, modification or removal of sensitive information maintained by Church Lawton School, specifically through the use of removable media.

This policy refers to all types of computer storage which are not physically fixed inside a computer and includes the following:

- Memory cards (like those used in cameras), USB pen drives etc.;
- Removable or external hard disk drives;
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player);
- Optical disks i.e. DVD and CD;
- Floppy disks;
- Backup Tapes;
- Personal Cloud accounts **including but not limited to** DropBox, GoogleDrive. iCloud.

This policy also covers all data including:

- Data stored on a share internally and externally;
- Teaching and learning data;
- Administration and management information data.

Policy

1. The use of removable media is prohibited within the School computer domains, ***unless agreed in writing for critical purposes, in which case, the below applies.***
2. If data is required to be transported via removable media please seek advice from IT Helpdesk.
3. Removable media used to store data shall only be used by staff who have an identified and business need for them.
4. Any sensitive or highly sensitive data transferred to a removable media device must remain encrypted and must not be transferred to any external system in an unencrypted form.
5. Data stored on removable media is the responsibility of the individual who operates the devices.
6. Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.
7. Mobile devices and/or removable media that have become damaged should be handed back to local IT helpdesk to ensure it is disposed of securely to avoid data leakage.
8. If a member of staff who used a mobile device and removable media was to leave, they should return the devices to IT Helpdesk for secure destruction and/or redistribution.

Use of removable media is recorded centrally by our systems. Unauthorised use of removable media may result in disciplinary action leading to dismissal.

Email Use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of email within the School. These policies are in addition to those already set out in sections that apply across the entire range of the School's computing and telecommunications facilities.

The most common method of virus transmission into computing systems is via email. You should always be suspicious of attachments that arrive unexpectedly even if they appear to come from someone you know. If in doubt, don't open the message and contact the IT Helpdesk immediately.

You should be aware that email messages carry the same weight in court as printed letters on Society letterhead. Thus, ill-considered messages could have serious repercussions. For example, you may be held to account for making defamatory remarks via email. A defamatory statement is one that tends to damage the reputation of another individual or organisation.

You must not participate in office gossip and/or spreading rumours over the email system about clients, customers, staff, contractors, competitors – in short, everyone. Even if it may seem innocent to you, it may give rise to liability for defamation by both you and the School. The School by its very nature gives a great deal of advice to a wide range of people – that advice is obviously given through its staff. You will know whether or not it is part of your duties to give advice via email and the extent of your authority to do so. If you are acting within the normal course of your duties and your expertise, and you act in good faith without malice or capriciousness, then you will be protected even if your advice proves to be wrong. However, if you act outside your competence or outside your authority then again you may be liable for any harmful consequences of your actions. If you are asked to give advice in email, and you are unsure whether or not you are competent to give it, then don't - at least not without seeking advice yourself. Never give gratuitous advice on an area that is not within your expertise; you may be liable to any third party who relies upon it to his/her detriment, not just the person to whom you addressed it.

Do not enter into contractual commitments by email without legal advice. Email is capable of forming or varying a contract in just the same way as a written communication. Because of the perceived informality of email, there is the danger of contracts being inadvertently formed by employees, to which the School is then bound.

You must comply with the following rules before entering into contracts by email:

- You must obtain authorisation before negotiating contracts by email. You must take advice from your manager before entering into contractual commitments. Managers should always seek advice from the School Business Manager;
- You must include the statement “subject to contract” in all emails if you conduct contractual negotiations via email until such time as it is intended that a binding contract should come into existence;
- You must be satisfied of the legal identity of the other contracting party before entering into a binding contract via email.

Email Etiquette

In addition to the above rules, the following guidelines should be followed when using the email system:

- Always maintain a professional image. Ensure the style, tone and content of emails is appropriate;
- Do not use email for urgent messages. Use the telephone. It should be noted that the delivery and integrity of email cannot be guaranteed;
- Respond to emails in a timely and professional manner. Always acknowledge receipt of emails requiring responses even if you cannot reply fully straightaway;

  Send emails only to those recipients/groups for whom the message is intended; Refrain from the use of BCC except where recipients email addresses need to be protected under GDPR;
- Ensure the subject matter is clearly indicated in the heading;
- Try to use plain text in emails. Fonts, underline, colour, graphics and tables not only add to the message size, slow systems down and may adversely affect delivery times but may also be lost in external emails;
- Limit the number and size of your file attachments as they result in increased traffic around the School's network and may incur the displeasure of external correspondents if they must pay to be connected whilst downloading the resulting large email message;
- Avoid sending trivial messages, jokes, gossip or adverts by email;
- Know that the School reserves the right to limit absolute message sizes allowed into or out of its email network;
- Identify your contact details in emails;
- Re-read and spell check messages prior to sending to ensure accuracy and clarity;
- Read and delete emails regularly;
- Remember to activate your Out of Office Assistant when you are away for more than a day – this way others will know you are not actively reading your email;

Email messages can be impersonal and/or misinterpreted so when sending an email consider whether it is the most effective method of communicating in that situation.

Internet Use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of the School's Internet facilities. These policies are in addition to those already set out in sections that apply across the entire range of the School's computing and telecommunications systems. The School encourages authorised staff to access the Internet during working hours, when direct work-related benefits can result. However, there are limits to personal use of the Internet, which are set out elsewhere. You should note:

- Different access for different types of personnel may be given;
- The School reserves the right to block access to certain Internet sites;
- Internet sites that are cost related or have cost implications in their terms of access must not be subscribed to without the prior authority of the relevant budget holder;
- Without prior approval from the IT Department, you may not download software or files from the Internet for use on the School's systems;
- Any such software or files that are approved for download via the Internet become the property of the School and may be used only in ways that are stipulated by their licences or copyrights and in a manner consistent not only with this policy but with the requirements outlined by the IT Department;
- Excessive personal use of the Internet during or outside business hours is not allowed;
- Downloading entertainment software or games or playing games against opponents over the Internet or Intranet at any time is forbidden.

Do not download, store, reproduce or distribute documents, pictures, logos, music or works of others without the owner's permission as this may infringe copyright laws. If you download articles and other materials from the Internet, you must remember that you need permission from the author before using such information for business purposes.

The dissemination of copyrighted information is a disciplinary offence which may result in disciplinary action being taken against you including in serious cases dismissal. If in doubt, speak to your manager about whether a particular work is copyrighted. Managers may seek guidance from the Company Secretary if necessary.

Supplementary Information

Supplementary Information: Summary of Acceptable Use of ICT

The School provides computer and telecommunications systems for use by employees in support of its activities. All users are responsible for ensuring that these systems are used in a professional, ethical and lawful manner. Therefore, it is important to define acceptable use principles to protect the staff, the school and the information itself.

This document is intended as a summary of your responsibilities as an employee, as defined in the school's Acceptable Use of ICT document, which forms part of your contractual Terms & Conditions. Further information on General Data Protection Regulation 2018 can be found in the NASAT and NAS Data Protection Policy documents. Both of these documents are available from your Line Manager.

IMPORTANT All users of the schools computing and telecommunications systems may be monitored, as circumstances warrant. Infringement of this policy may give rise to appropriate disciplinary measures. If you are not certain you fully understand and can comply with this policy you should seek further clarification from your Line Manager.

General
Limit personal use At your manager's discretion, occasional personal use of email, internet and telephone systems is permitted as long as it does not interfere with staff productivity or responsibilities and does not incur costs. **Manage your virtual space** Virtual space, like office space, is finite and expensive. Delete files or email messages you do not need anymore. Avoid keeping multiple copies of files unless absolutely necessary. **Only use software & hardware authorised by the IT Department** To prevent copyright infringements and damage to school systems, all computing equipment (including laptops, phones, iPads and printers) must be authorised by the IT department before being used with school systems. Similarly, all software (including logos, games and video/music files) must also be authorised by the IT department before being used with school systems. Do not use, without prior written authorisation, removable storage or personal devices. **Help your colleagues** Activate your Out of Office Assistant when you are away for more than a day – this way others will know you are not actively reading your email. Also, think about whether sending an email is the most effective method of communicating. **Help the IT department to help you** Notify the IT department of any IT related matters as soon as you can. This includes information regarding staff that are starting or leaving, as well as any temporary workers that require access to the IT systems. **Do not give out personal details** Do not give out personal information to pupils such as your mobile telephone number and personal email address. **Images of pupils** Images that contain pupils must only be taken, stored and used for professional purposes in line with the school Code of Practice (available from your line manager or HR) and with the written consent of the parent, carer, member of staff or Principal. **Staff and Student Laptops** Staff laptops are encrypted for data security. Staff must not use Pupil laptops for professional work or viewing of their emails. Staff must not sign in using their credentials to a student laptop for a student to use. **Personal Data** Personal data is only to be used for the purpose intended in our DP Policy, and data must be kept securely and only on school based systems. This data is to be used appropriately in school, or through school provided, secure remote access.

IT Security

Keep your password secret. Do not write it down and do not give it to anyone – even someone from the IT department. If you think someone else knows your password, you should change it immediately. If you need to give a colleague access to your work, please contact the IT Helpline for advice. Change your password every 30 days.

Do not use a password that you have used before, and do not use passwords that are obvious or easy to guess. Lock your workstation when you are away from it Lock your workstation by pressing CTRL-ALT-DEL followed by ENTER. Keep IT safe IT equipment is expensive and fragile. Make sure you take all reasonable precautions to protect it from damage and theft.

Do not use, without prior written authorisation, removable storage devices or personal devices.

Email & Internet

Never send confidential information via email. Email is neither private nor secure. If you need to email confidential information, contact the IT Helpline for advice. Email can be legally binding. Never put anything in email that you would not be prepared to put on letterhead and sign. Remember, in court a piece of email is treated the same as a printed document. If you are unsure ask the Business Manager for advice.

Always be suspicious of attachments that arrive via email. This is especially true of anything you do not expect to receive, even if it appears to come from a well-known source. If in doubt, don't open it. Contact the IT Helpdesk for advice.

Use the Internet and email facilities appropriately. Do not view, download, save or transmit offensive, pornographic, or any other inappropriate material. Similarly, do not use copyrighted material without the owner's permission. Inappropriate use may lead to summary dismissal as well as being reported to the police.

E-Safety - an Overview

Students at NAS Academies Trust Schools have the right to access new and emerging technologies as part of their education and care. These technologies are a vital part of the lives of many people with autism and the school is committed to promoting students' development of the skills, knowledge and understanding to communicate, create, investigate, play and relax online. The school provides technology for students as well as providing a network that allows them to use their own devices.

NAS Academies Trust recognises that online activity brings with it potential risks including (but not limited to):

- accessing inappropriate content
- predatory behaviour and grooming
- sexting
- radicalisation and/or extremist behaviour
- bullying and threats
- identity theft
- financial harm
- corruption or misuse of data

Our primary aim with regard to E-Safety is to give students the ability to stay safe online – both inside the school and beyond. We aim to do this through education, embedding E-Safety in every aspect of the curriculum and working with parents/carers, siblings and others to promote safe use of technology. Please refer to the NASAT E-Safety Policy (and the associated procedures), available on the school website which lays out the ways in which we keep students safe while providing this education.

Aims

NAS Academies Trust Schools aim to provide students with the skills, knowledge and understanding to keep themselves safe online within the school and beyond, now and in the future. This policy gives guidance on providing a safe environment in which students may develop their own e-safety skills and sets out the expectations of NAS Academies Trust in relation to e-learning in its schools.

E-Safety Coordinator

Each school has a named member of staff with day to day responsibility for e-safety. This role may be combined with the Child Protection Officer role. This is primarily a safeguarding role, not a technical role, although the coordinator should have a good understanding of technical issues. The E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority as appropriate
- liaises with IT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant meetings and committees of Governors
- reports regularly to the Senior Leadership Team

The Principal is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as appropriate and receive regular monitoring reports from the E-Safety Coordinator and act on them accordingly.

In the event of a serious e-safety incident occurring, Appendix 1 of the E-Safety Policy should be followed.

Staff

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and procedures.
- They report any suspected misuse or problem to the E-Safety Coordinator for investigation.
- Digital communications with students (for example by email or through the Virtual Learning Environment) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- They help students understand and follow the school e-safety and acceptable use policy
- They strive to ensure students have an understanding of behaving legally and responsibly online
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, tablets, games machines, cameras and other devices and that they monitor their use and implement current school policies with regard to these devices

Students

NAS Academies Trust Schools will attempt to give students the knowledge, skills and understanding to keep themselves safe online, both in the school and outside it.

- Students are responsible for using ICT systems in accordance with the student Acceptable Use Policy, which they will be expected to sign before being given access to school systems. For some students it may be expected that parents/carers would sign on behalf of the student.
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to go about doing so. As far as possible students will be expected to know and understand school policies on the use of mobile phones, tablets, games machines, cameras and other devices.
- Students should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The NAS Academies Trust is aware that parents and carers may not fully understand technical issues and be less experienced users of ICT than their children. Parents/carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what to do about it. The school will therefore take every opportunity to help parents understand these issues through collaborative working and training, which may include siblings or other family members as appropriate. Parents/carers are responsible for:

- working with the school to ensure that their children have the best opportunity to learn to keep themselves safe online
- signing the student Acceptable Use Policy (if necessary)
- accessing the school's online resources in accordance with the relevant school policies

Criteria for Success

- There is clear evidence that staff understand and act on the e-safety policy. This may come from assessment of staff after training, review of incident logs and 'white hat' security testing. It is the responsibility of the E-Safety Coordinator to collect this evidence and of the E-Safety Governor and the Principal to evaluate it.
- Students are able to demonstrate increased understanding of e-safety issues through formal and informal assessments.
- Information on incidents show that they are being reported appropriately and that incidents are followed up.
- This policy is reviewed and revised according to the set timescales.
- The school uses tools such as the SWGfL 360 Degree Safe self-assessment to review e-safety provision and identify possible improvements.

If you have any questions regarding this document, please contact the IT Support Desk at support@naschurchlawton.cheshire.sch.uk

All Staff are required to sign to acknowledge receipt and understanding of this policy (Appendix included in Staff Welcome Pack)