Policy- E-Safety

IT Services

Principal: Mr S Strickland – BA (Hons), MA, NPQH

Berrywood Road, Duston
Northampton NN5 6XA
Telephone Nos. **01604 460004**

Email: letters@thedustonschool.org / **www.thedustonschool.org**

Contents

Introduction

1.1 Policy Statement

This policy is written to meet with the template & recommendations of Northamptonshire county council & Ofsted (links below)

- ***http://www.northamptonshire.gov.uk/en/councilservices/EducationandLearning/services/e-safety/Pages/Making-my-school-esafe.aspx***
-

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. However the below must be considered.

- E-Safety is a **child protection issue not an ICT issue**.
  All people working in a school, whether adult or child have a duty to be aware of e-safety at all times, to know the required procedures and to act on them please see relevant 'Acceptable use policy' (below)
- E-safety is not limited to school premises, school equipment or the school day. Neither is it limited to equipment owned by the school.
  E-safety is a partnership concern. (An incident occurring outside the school and brought to the schools attention will be treated as if it had happened on school premises in the teaching day)

1.2 Duty Of Care

- A designated member of SLT has responsibility for all child safety and therefore e-safety matters.
- A designated member of SLT has accountability for this policy and responsibility to annually review and update it's contents. This will then be agreed and signed off by the Principal and school governors.
- The school should allocate internet access to staff and pupils on the basis of their educational need.
- At primary level pupil usage should be fully supervised.
- All staff have a responsibility to support e-Safe practices in schools.
- Children at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach e-safety protocols. (Please see student acceptable use policy)
- Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. A designated member of SLT has accountability for data protection and there is a separate data protection policy.

"It is advised students sign an acceptable use policy at the start of the academic year.

Also encourage parents to sign an acceptable use policy on the internet on behalf of their son or daughter encouraging safer internet use and endorsing the schools boundaries." (Northampton County Council)

1.3 Scope

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on the school premises and outside. This must include staff or pupil personal devices such as mobile phones and tablets which have been brought onto school grounds. The policy must also take into consideration devices the school has issued members of staff and pupils to use on and off site.

At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Non functional points include

- E-safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks.
- Children being taught safe practices and that the safety policy will be monitored and enforced.
- The e-Safety policy links with the school Acceptable Use policy.
- E-Safety covers technology not owned by the school. For example a school would respond to e-Safety threats involving members of their community whether they

occurred during the school day, on the school site or if perpetrated using equipment not owned or operated by the school.

1.4 Local Council Guidelines

- The e-safety policy will be distributed and discussed with all members of staff.
- Also the policy will be easily accessible for the school community.
- To protect the school community the school will implement acceptable use polices.
- Staff, students and parents will be made aware that internet access is monitored and can be traced back to an individual's account.
- Up to date and appropriate training for staff in e-safety is provided at least every 12 months this can be sought through Northamptonshire County Council's e-safety advisor.
- Members of staff who manage filtering systems or monitor ICT use will have clear procedures and will be appropriately supervised by SLT for reporting issues.
- The school will make use and cascade useful e-safety resources out to the school community.
- All pupils primary, secondary, staff and parents need to be made fully aware of the risks that go with social networking sites.

2. Monitoring

Authorised ICT staff and relevant SLT members may:

1. Inspect any ICT equipment owned or leased by the school at any time without prior notice. a. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department.

   b. Any ICT authorised staff member will be happy to comply with this request.

2. Monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

3. Without prior notice, access the e-mail or voice-mail account where applicable, of

someone who is absent in order to deal with any business-related issues retained on that account.

4. Review, record and issue CCTV footage of the activity in public corridors of the school.

5. Monitor and review internet activity from end user device to activity logged with the internet provider.

3. Breaches

- A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

- For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

4. Acceptable Use Policies

4.1 AUP- STUDENT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I will only use ICT systems in school, including the internet, e-mail, digital video, and

mobile technologies for school purposes.

- I will not download or install software on school technologies.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- For school work I will only use my school e-mail address.
- I understand that the school will monitor my use of the ICT systems, email and other digital communications and this info can be made available to my teachers.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will be responsible for my behavior when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone external to the school community unless this is approved by my teacher.
- I am aware that when I take images of pupils and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school.
- I will not disclose or share personal information about myself or others when on-line.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- I will not attempt to bypass the internet filtering system..
- I will respect the privacy and ownership of others' work on-line at all times
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.
- I understand that mobile phones and smart watches are not permitted at the Duston School.
- I will not sign up to online services until I am old enough to do so.
- I will only use my personal devices (Laptop/tablet) in school if I have permission and have signed the BYOD Acceptable Use Policy. I understand that, if I do use

my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Dear Parent/ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with school **safeguarding officer.**

Please return the bottom section of this form which will be kept on record at the school

--✂--

Parent/ carer signature
We have discussed this document with……………………………………………..(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at The Duston School.

Parent/ Carer Signature …….……………………….……………………….

Pupil Signature………………………………………………………………………..

Class …………………………………. Date ………………………………

4.2 AUP- STAFF, GOVERNORS & VISITORS

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the **safeguarding officer.**

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS or financial software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick.
- I will not install any hardware or software without permission of IT services.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Executive Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, SLT or Executive Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm. Exceptions being in offices and the staff rooms.
- Staff employed by the school should not accept students as friends past or present on social media accounts.
- Staff posting inappropriate comments and media on social media could lead to disciplinary action and having their employment terminated.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted
- I understand this forms part of the terms and conditions of my employment.

Staff Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …….…… Date ……

Full Name ……..…….(printed)

Job title .....

5. Specialist Areas

5.1 Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

5.2 Cyber Bullying

Cyberbullying is best defined "The use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else". DCSF 2009

- Bullying is not a specific criminal offence in the UK whereas types of harassing or threatening behaviour or communications could be a criminal offence.

- As per Ofsted requirements all incidents of cyberbullying are recorded and reported to the safeguarding officer.

- The school community are aware that they must keep any evidence of cyberbullying such as print out, screen shots and photos.

- Digital Media must be viewed on the designated computer held in ITservices then stored only on that device.
- The school community are aware that they must keep any evidence of cyber bullying such as print out, screen shots and photos.

- The school will take a number of steps to identify the bully. This could well mean going through the schools monitoring/filtering system to see what has been sent. Victims and perpetrators may have to be interviewed and the police may have to be involved if necessary.

- Parents, staff and pupils are required to work with the schools to support the schools approach to cyber bullying.

Sanctions for those involved in cyber bullying:

- The perpetrator will be asked to remove material deemed inappropriate or offensive.
- The service provider can be contacted and asked to remove the content, however, if reporting something on a social network site it may be necessary to check if it has broken their terms and conditions.
- Internet access may be suspended for the perpetrator/s for a period of time and other sanctions put in place in accordance with the schools behaviour or e-safety policy.
- Parent and carers will be informed.
- The police may be contacted if there is a suspicion that a criminal offence has been suspected.

5.3 Staff Social Media

Staff have the right to work free from harassment and bullying themselves that has been carried out over the internet. DFE guidance published in 2014 states that schools should also encourage all members of the school community including parents to use social media responsibly. (Northampton County Council)

- It is highly recommended that staff familiarise themselves with the security and privacy settings on social media accounts. Please see Facebook privacy process in appendices.
- Staff employed by the school should not accept students as friends past or present on social media accounts as this could leave the member of staff/s open to bullying and harassment. It's recommended they also do not have online friendships with parents publically acknowledged. (this is reflected in the AUP)
- Staff posting inappropriate comments on social media could lead to disciplinary action and having their employment terminated. (this is reflected in the AUP)
- If a member of staff has been bullied online or is being bullied online it should be reported immediately to a line manager or senior member of staff. If possible try and keep any evidence and record the date and time.
- If the perpetrator is known to be a current pupil or colleague the most effective way to deal with it is through the schools disciplinary procedures. (please see incident reporting)

5.4 Staff/Sixth Form Bring Your Own Device (BYOD)

- All BYOD users must obtain an acceptable use agreement that is signed and dated
- The network will be secure and clearly differentiated by policies on the SSID (different Wi-Fi networks according to users).
- The devices will be covered by the schools filtering system whilst being used on the premises.
- Regular audits are carried out to ensure staff are complying with the AUP.
- Any user leaving the school will be made clear what is expected of them and their device before they leave.

5.5 Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The school gives relevant staff access to its Management Information Systems including SIMS, PS financials with a unique username and password.
- Staff should be aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the 'Policy for Acceptable ICT Use'.
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the school:

- What information is held, and for what purposes.
- What information needs to be protected, how information will be amended or added to over time.
- Who has access to the data and why.
- How information is retained and disposed of.

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a secondary school, there may be several individuals, whose roles involve such responsibility.

It should be clear, however, to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Data Ring Fencing

- IT-services provides a service of data encryption and ring-fencing key data such as financial and HR records.

5.6 Disposal of Redundant ICT equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen (WEE certificate).

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 1998
  https://ico.org.uk/for-organisations/education/
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

- The school's disposal record will include:
  - Date item disposed of.
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of eg waste, gift, sale.
  - Name of person & / or organisation who received the disposed item.

* If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

https://ico.org.uk/

Data Protection Act – data protection guide, including the 8 principles

https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

5.7 Email

"The school email system should not be considered as completely private and many schools, as do businesses, reserve the right to monitor email." (Northampton County Council)

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value.
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.

- All pupils have their own individual school issued accounts.

- The forwarding of viral chain emails is not permitted in school. However the school has set up a support account, itservices@thedustonschool.org, to allow pupils to forward any chain emails causing them anxiety. No action will be taken with this account by any member of the school community

- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.

- Staff must follow the incident reporting process if they receive an offensive e-mail.

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

    - School e-mail is not to be used for personal advertising.

    - Sensitive data emails:

        - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
        - Verify the details, including accurate e-mail address, of any intended recipient of the information.
        - Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
        - Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

5.8 Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

All internet use through the Lightspeed tooling is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services before use.
- IT services Must be given at least 2 weeks to review and test a piece of software before it can be distributed.
- Searching for images through open search engines is discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- You must not post personal, sensitive, confidential or classified information or disseminate such information in. any way that may compromise the intended restricted audience
- On-line gambling or gaming is not allowed.

It is at the Executive Principal's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- The Duston Trust has a monitoring solution via Lightspeed and HP IMC where web-based activity is monitored and recorded.
- School internet access is controlled through Lightspeed filtering service.
- The Duston Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/

closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ***(technician/teacher)*** for a safety check first.

- Pupils and staff are not permitted to download programs or files on school based technologies.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed via email.

Online Technologies

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

- Our pupils are asked to report any incidents of cyber bullying to the school.

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the SLT.

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

5.9 Password Policy

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you aware of a breach of security with your password or account inform IT services immediately.**
- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 2 weeks.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is

15 minutes.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).

- In our school, all ICT password policies are the responsibility of **The IT systems manager** and all staff and pupils are expected to comply with the policies at all times.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.

- Prompt action on disabling accounts will prevent unauthorized access.

- Regularly change generic passwords to avoid unauthorised access.

5.10 Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important with shared printers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.
- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential or classified data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Please refer to the document on the grid for guidance on How to Encrypt Files

- http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

5.11 Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

5.12 Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. HCC guidance can be found:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

Publishing Pupils' Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- Parents automatically agree to this in the home-school agreement that they sign when they start the school and have the option to **opt out** of the photos being published.
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

- Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

- Only the digital team has authority to upload to the internet.

For further information relating to issues

http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

The Duston Trust enforces the following policies:

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Executive Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Executive Principal.

- Pupils and staff must have permission from the Executive Principal before any image can be uploaded for publication.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Storage of Images

- Images/ films of children are stored electronically on the school's network and only accessible by staff. Printed images of students for use in teachers' standards folders must remain in the staff member's possession or stored in a locked cupboard when not in use.

- Pupils and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Executive Principal.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

5.13 Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the guidance team, IT services and SLT.
- We do not use publicly accessible webcams in school.
- Webcams will not be used for broadcast on the internet without prior parental consent:
    - Misuse of the webcam by any member of the school community will result in sanctions.
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

For further information relating to webcams and CCTV, please see
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- Approval from the Executive Principal is sought prior to all video conferences within school to end-points beyond the school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

For further information and guidance relating to Video Conferencing, please see

http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

5.14 Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Protecting Personal or Sensitive information' section.

- Always consider if an alternative solution already exists.
- Encrypt and password protect.
- Store all removable media securely.
- Removable media must be disposed of securely by your ICT support team.

5.15 Servers

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Backup tapes should be encrypted by appropriate software.
- Data must be backed up regularly.
- Backup tapes/discs must be securely stored in a fireproof container.
- Back up media stored off-site must be secure.

6. Incident Reporting

In the event of suspicion, all steps in this procedure should be followed

- Have more than one senior member of staff/volunteer involved in the process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer (housed in IT services) that will not be used by young people and if necessary can be taken off site by the police should the need arise. Ideally use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also the sites and content visited are closely monitored and recorded this will provide further protection.

- Make sure you record the URL of any site containing the alleged misuse and describe the nature of the content causing you concern. If possible record and store screen shots of the machine were the incident has taken place. The information collated should be printed out, signed and dated.

- One this has been completed and fully investigated the safeguarding team and e-safety team or lead will need to judge whether the concern has substance or not. If it does then appropriate action will be required and could include the following:

    - PCSO/Police referral

- Referral to the MASH team (When there are child protection concerns)
- CEOP
- CSE toolkit – To look at the risk of CSE

6.1 E-Safety Poster

- To be displayed throughout the school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

- If there are any concerns around on line grooming this includes images of child abuse the Police should be contacted immediately.

  Other circumstances when e-safety concerns should be reported to the Police one discussed with the designated safeguarding officer are highlighted below:

  - Radicalisation – Further information on prevent contact the Northamptonshire police- mail@northants.police.uk
  - http://www.northamptonshirescb.org.uk/Online Grooming
  - Hacking
  - Hate Crimes
  - Harassment
  - Certain types of adult material
  - Other criminal conduct, activity or materials

How will e-safety complaints be handled?

Parents, teachers and pupils should know how to use the schools complaints procedure. The facts of the incident or concern will need to sort and all evidence needs to be compiled where possible and appropriate. E-safety incidents may have an impact on pupils; staff and the wider community both on and off site can have legal and disciplinary consequences.

Other situations could potentially be very serious and a range of sanctions may then be required, which should be then linked to the school disciplinary policy. Safeguarding or illegal issues must be referred to the school safeguarding officer or e-safety coordinator. Advice on dealing with illegal use should be discussed with the Police.

Appendices

http://www.northamptonshire.gov.uk/en/councilservices/EducationandLearning/services/e-safety/Pages/Making-my-school-esafe.aspx

Staff Responsible	TWI		
Date approved by GB:	17/03/16	**Review Date**	March 2019