High March

ICT Security Policy

Policy written by:	Mrs Julia Halford
Person responsible for latest revision:	Mrs Julia Halford and Mr Mike Wright
Page number of any significant changes in latest revision:	Pages 4-5
Date of latest circulation to staff:	March 2019
Date of next review:	March 2020

ISI Reference	7h

This policy applies to the Early Year Foundation Stage, Key Stage 1 and Key Stage 2

Useful Websites	
www.education.gov.uk	
www.childnet.com	
www.thinkuknow.co.uk	www.swgfl.org.uk/resources
www.saferinternet.org.uk	www.gooseberryplanet.com

High March

ICT Security Policy

The Internet and other forms of digital information are powerful tools. These technologies can stimulate discussion, encourage creativity and promote effective learning. As a result, they have become an integral part of the education environment.

The Proprietors have ultimate corporate responsibility for ensuring that the School complies with the legislative requirements relating to the use of information and ICT security and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headmistress.

The Headmistress is responsible for ensuring that the legislative requirements relating to the use of information and ICT system security are met and that the School's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the School. The Headmistress is also responsible for ensuring that any special security measures relating to the School's information or ICT facilities are applied and documented as an integral part of the Policy. (Please see the Data Protection Policy and Privacy Notice for Staff). The DPG supported by the Data Protection Audit Committee is also responsible for ensuring the requirements of the GDPR are complied with fully by the School. In addition, the Headmistress is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy.

All staff change their network passwords once a year. Passwords are a minimum of 8 characters and must contain at least one capital letter and one number. The network is configured to force an annual password change and the Network Manager monitors this. Engage passwords are also changed each year. The Network Manager implements the forced password change for Engage. The passwords for Engage are a minimum of 12 characters, with at least one upper case letter, at least one lower case letter, at least one number and at least one special character. The Network Manager gives guidance on the minimum requirements.

The objectives of this Policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure users are aware of and fully comply with all relevant legislation.
- Ensure staff understand the need for information and ICT security and their own responsibilities in this respect.
- Ensure pupils have safe and secure internet access.

Monitoring

High March pupils should have an entitlement to safe internet access and to ensure this happens the School has a robust web content filter. The School also has a system of firewalls and antivirus software to make sure that the High March ICT Network is as secure as possible. In addition to this, the School operates a software package called Impero, which automatically monitors keystrokes searching for safeguarding trigger words and phrases. If a trigger is activated, a screen shot is taken and the Network Manager is alerted. The Network Manager records all such attempts. Each week a summary of critical alerts is emailed to the Headmistress. If necessary, the Head of ICT speaks to any child involved to ascertain the situation.

Staff ICT Acceptable Use

To guarantee that all members of the High March community are safe when using ICT we expect all staff to follow a simple set of rules. These rules are laid down in a Staff ICT Acceptable Use Policy. Signing this document forms part of the High March induction process and confirmation that Data Protection Induction has taken place. A signed copy is kept on each member of staff's personal file. (See Appendix 3)

Social Networking Sites

Some staff may use social networking sites for personal use in their own time. If so, staff should ensure their passwords are strong and secure at all times. Profiles and photos of staff should be 'locked down' as private so that pupils or parents do not have access to personal data or images.

Staff leave themselves open to a charge of professional misconduct if images of themselves or other members of staff in a compromising situation are made available on a public profile by anyone.

If parents or pupils gain access to the profile of a member of staff by fraudulent means (impersonation or hacking) the Headmistress should be informed immediately.

In some cases, friendships exist between staff and parents at the school. In these instances, social networking is acceptable, but caution must be exercised so that professional standards are maintained and staff do not compromise themselves or the School.

The Internet

Under no circumstances should adults in the School access inappropriate images. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material, is illegal and, if proven, will invariably lead to the individual being barred from work with children and young people.

Using School equipment to access inappropriate or indecent material, including adult pornography, will be reported to the police immediately. Such action will lead to immediate suspension and possible dismissal, particularly if, as a result, pupils might be exposed to inappropriate or indecent material.

Communication with Pupils

- Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites, social networking sites, online gaming and blogs. (Please see the Mobile Phone and Camera Policy.)
- Staff should never share any personal information with a pupil and they should ensure all communications are transparent and open to scrutiny.
- It is important for staff to be circumspect in their communications with pupils to avoid any possible misinterpretation of their motives or any behaviour that could be construed as grooming. Staff must never store images of students on personal cameras, devices or home computers.
- No member of staff should share personal contact details with pupils, including email, home or mobile telephone numbers, unless the need to do so is agreed with the Headmistress and parents of the pupil concerned. Occasionally children need to email homework to the School, (for example, if their printer is broken). The pupils are told to ask their parents to send the email rather than the child using their personal account. If the child does use their account, the member of staff should not reply.
- Email or text communications between staff and pupils outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based websites, such as social networking or instant messaging.

Pupil ICT Acceptable Use

To maximise the safety of all members of the High March community when using ICT, we expect all pupils to follow a simple set of rules. Each September the Responsible Use Policy is distributed. Parents and pupils are required to sign the policy form, indicating that they have read and understood it together. The Responsible Use Policy is also read with classes during ICT lessons in September. The teachers of the Junior House pupils ensure that it is adhered to within their lessons.

This Responsible Use Policy (see Appendix 1) is intended to ensure:

- That pupils will be responsible users and stay safe while using the Internet and other communication technologies in school.
- That School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The School will ensure that the pupils have supervised access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. The Head of ICT has overall responsibility for this.

Cyber safety is taught to each year group on an annual basis. In Reception this is discussion-based and includes using the Internet at home. In Years 1 to 6 the topic is covered at the beginning of the Autumn Term. This is to ensure that the pupils are fully aware of how to use the Internet responsibly. Where it is age appropriate, this will include considering the long-term implications of any content posted online. Also the importance of reading and adhering to any website's terms of conditions of use, including those around

age restrictions, will be impressed upon the pupils. A letter outlining the content of the lessons is then issued to parents.

Cyber Bullying

Cyber Bullying is unacceptable and how to deal with Cyber Bullying is covered when studying internet safety. Pupils are taught to keep any evidence of Cyber Bullying and it will be dealt with in line with the School's Anti-Bullying Policy.

Instances of Cyber Bullying are recorded on Engage and noted on the separate bullying log held by the Head of Junior House and the Deputy Head (Pastoral).

The Network Manager ensures that the firewalls, privacy settings and other safeguards are in place. The Network Manager is the point of contact in the School for E-safety. He is available to be called throughout the day in an emergency.

Parental Awareness of Online Safety

It is important for parents to be aware of online safety. Each year the Head of ICT writes to parents of Year 1 to Year 6 when the topic of Cyber Safety has been completed. This letter reminds the parents of the importance of being vigilant about their child's use of devices. A list of useful websites is included in this letter. The Headmistress also writes to parents of Year 6 to remind them of the age limit for social networking sites. Appendix 2, an Online Safety Guide for Parents, is sent to parents during the week of Safer Internet Day in February.

Prevent Duty

The School also has regard to the guidance in the following document:

Prevent Duty Statutory Guidance: for England and Wales under s29 Counter-Terrorism and Security Act 2015

Prevent is supplemented by non-statutory advice and a briefing note:

- The Prevent Duty: Departmental advice for schools and childminders (June 2015)
- The use of social media for on-line radicalisation (July 2015)

All staff are required to have due regard to the need to prevent children and adults from being drawn into terrorism and to prevent radicalisation and extremism. This part of our Policy should be read in conjunction with our Child Protection and Safeguarding Policy and our SMSC Policy. All staff should be vigilant and alert to pupils attempting to access online and via "apps" material that could be used in an attempt to radicalise children.

Extremism is defined as "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. Included

within the definition of extremism are calls for the death of members of our armed forces, whether in this country or overseas. The most significant threats are currently from terrorist organisations in Syria and Iraq, and Al-Qaeda associated groups. However, terrorists associated with the extreme right also pose a continued threat. We have no place for extremist views of any kind at High March. Our pupils see High March as a safe place where they can explore controversial issues safely and where our staff encourage and facilitate this. As a School, we recognise that extremism and exposure to extremist views can lead to poor outcomes for children and hence should be treated as a safeguarding concern. High March staff will challenge extremist views in order to protect our pupils.

All High March employees completed on-line Prevent training in 2016 and new employees are required to complete this on appointment.

The Head of ICT in conjunction with the Network Manager is responsible for checking that no terrorist or 'grooming' organisations contact or are able to access pupils.

Related Documents

- Anti-Bullying Policy
- Child Protection and Safeguarding Policy
- Critical Incident Policy
- Curriculum Policy
- Data Protection Policy
- ICT Handbook
- Mobile Phone and Camera Policy
- Privacy Notice for Staff
- SMSC Policy

APPENDIX 1

Responsible Use Policy

The following rules help to keep you safe and respectful of others when using computers on the High March network.

General Rules

- ✓ You should only use the computers in school for schoolwork and homework.
- ✓ Take care of the hardware: keyboards, headphones, mice, monitors, cables etc.
- ✓ No food or drink should be taken into either of the ICT suites or consumed near a computer.
- ✓ Hands should be clean when using the keyboard and mouse.
- ✓ Leave the areas around the computers tidy and remember to remove your belongings.

Using the computers

- ➢ Only access the network using your own username and password: do not use anyone else's.
- ➢ Do not try to access other people's files.
- ➢ When using the Pupil drive be careful not to delete other people's files or documents.
- ➢ Do not attempt to install programs or applications on the school computers.

Printers

- ❖ Always ask a member of staff before printing your work.
- ❖ Check that work is finished and you have checked the spelling before printing.
- ❖ Only print the pages you need.
- ❖ Check you are using the correct printer before you press print.

Using the Internet

- ✦ You must ask permission from the supervising member of staff before accessing the Internet.
- ✦ You should only use the Internet for schoolwork and homework, unless permission has been granted for other use.
- ✦ Always behave in a responsible way when online.
- ✦ Report any unpleasant or upsetting material to a member of staff immediately as this will help protect other pupils.
- ✦ You must not try to access chat rooms or social networking sites from the school computers.
- ✦ Never share personal details about yourself such as full name, home address, school name, email or phone number with anyone else over the Internet.
- ✦ Do not download program files or applications to the school computers from the Internet.
- ✦ Understand that the School may check computer files and monitor the Internet sites you visit.

Parent name: _____ | Pupil Name: _____ Form: _____

Signature: _____ | Signature: _____ Date: _____

APPENDIX 2

Online Safety Guide for Parents

- Place the computer in a well-trafficked area in the home where the whole family can use it. Ensure mobile devices such as iPads have all the necessary safeguards.
- Monitor and establish rules for the amount of time spent online.
- Ensure you are making use of the different parental control tools that are available including protective software and controlled access.
- Use the Internet with your child and learn about the services your child uses.
- Talk with your child to agree what kind of sites she is allowed to visit.
- Don't let your child visit unmonitored chat rooms and monitor where she goes.
- Ensure your child never gives out personal information online.
- Ensure your child never, for any reason, agrees to meet someone face to face that she met online. Get to know your child's online friends.
- Talk to your child about cyber bullying.
- Be aware that social networking sites such as Facebook have a lower age limit of 13, but the site is unable to verify the age of applicants and thus disallow an underage user.
- Make sure your child knows to tell you about anything online that makes her uncomfortable, including unwanted emails or chat requests.
- If your child receives a message of a sexual nature or is threatened, contact your Internet Service Provider and ask for their help.
- Keep the webcam on your child's computer covered, unless required for Skype etc.

APPENDIX 3

Staff ICT Acceptable Use Agreement

I understand that working in an educational context brings with it high expectations of behaviour and integrity, and responsibilities with regard to safeguarding. These expectations include:

- Interacting with pupils in an appropriate way.
- Interacting with colleagues, parents, and other School or work contacts in an appropriate way.
- Being trustworthy with confidential and sensitive information.
- Looking after the fabric and equipment of the School and respecting school property.
- Maintaining the reputation of High March.
- Maintaining professional standards of conduct.

These things are equally true when ICT systems, including computers and phones are involved.

Staff may use the school equipment and network for:

- School / work purposes
- Reasonable personal use that does not interfere with work.

I understand:

- This agreement applies to the use of High March ICT systems regardless of location.
- There is a presumption that emails, voice messages and data are stored on High March equipment for business purposes. This information will be filtered and monitored, and may be accessed to meet business needs.

I will not:

- Do anything that may compromise the safety of children or staff.
- Disclose my username or password to anyone else.
- Try to use any other person's username and password for any purpose.
- Do anything offensive that might bring the School into disrepute. This includes using best endeavours to ensure that any postings or entries on any social media networking sites do not bring staff or the School into disrepute.
- Access, copy, remove or alter any other user's files without their explicit permission.
- Engage in any on-line activity that may compromise my professional responsibilities.
- Attempt to install programmes on a machine, or store programmes on equipment unless approved by the school.
- Try to circumvent security settings or content filters.
- Deliberately breach anyone's copyright.

I will:

- Bring to the attention of the ICT Department or a member of the Senior Management Team any ICT activity or material that may be inappropriate or harmful.
- Report any damage or faults involving equipment or software, however this may have happened, as soon as reasonably possible.
- As far as is possible, use High March provided systems to communicate with parents on school and pupil matters. I will maintain professional standards of conduct if I communicate with parents socially using personal phones, email or social media.
- Comply with the requirements of GDPR and the terms of the Privacy Notice for Staff

Information Security

I understand that I may have access to sensitive information about colleagues, families or pupils in our care. I will comply with High March's guidance on data protection and will keep sensitive information within the School's network. I will not send sensitive information via personal email accounts (Hotmail, Gmail etc.) or store it on:

- Un-encrypted USB sticks
- Personal devices (phones, laptops) or
- Personal cloud storage (OneDrive, Drop Box, etc.)

Images and Videos

In order to prevent allegations of inappropriate activities, I will not store images of pupils on my personal devices. Any images taken on personal devices (including EYFS) will be downloaded to the School's systems as soon as reasonably possible and the personal copy permanently removed.

Bringing Your Own Device

When I use personal devices in work, I understand that the same expectations of behaviour apply as if I were using School equipment.

I understand that if I fail to comply with this Acceptable Use Agreement, I may have my ICT access suspended and / or be subject to disciplinary action. A copy of this agreement is available on request. I understand a copy of this signed document will be placed on my personal file.

I confirm that I have read and will abide by the Staff ICT Acceptable Use Agreement.

Signed: _____

Print name: _____

Date: _____