THE HAWKSWOOD GROUP

2018-19

E-Safety

Approved by the Management Committee of Hawkswood Group

Chair of Management Committee: Mr Mark Morral

Date approved	May 2017	Management Committee
Date amended	July 2018	Safeguarding and Inclusion Lead
Amendments agreed	September 2018	Management Committee
Reviewed	Annually	Management Committee

The Hawkswood Group
Executive Head Teacher: Catherine Davies
The Hawkswood Centre | Antlers Hill, Chingford E4 7RT

Associate Headteachers:
Burnside PRU: Bridget Solecka
Hawkswood Therapeutic PRU: Linda McCaffrey
Hawkswood Primary PRU: Marie Gentles
Forest Pathway College: Carolyn Crampin
Alternative Provisions: Gabrielle Grodentz

E-Safety Policy

Introduction

This E-Safety policy recognises our commitment to e-safety and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the ever increasing digital world and outlines the steps we take to ensure this happens.

As part of our commitment to E-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

To support, this we have clear expectations of all staff and students and these are outlined in our Acceptable Use Agreement (Annex 1 attached) and named E-Safety co-ordinators in each PRU namely:

Hawkswood Primary PRU - Marie Gentles

Burnside Secondary PRU - Bridget Solecka

Forest Pathway College - Carolyn Crampin

Hawkswood Centre – Linda McCaffrey

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Management Team accepts the following responsibilities:

- Identify an E-Safety Co-coordinator for each PRU and support them in their work.
- Ensure adequate technical support is in place to maintain a secure IT system
- Ensure policies and procedures are in place to support the integrity of the school's information and data assets
- Ensure effective liaison with the Management Committee
- Make appropriate resources, training and support available to all members of the PRU community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout the school
- Ensure that all staff and pupils agree to and sign the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Be the first point of contact in school on all E-Safety matters
- Lead the school E-Safety team
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of PRU or AP staff , who makes use of the school IT equipment in any context, is made aware of the Acceptable Use Policy (AUP)
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on E-Safety issues to the Senior Leadership Team and Management Committee as appropriate.
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed E-Safety messages in learning activities where appropriate

- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Will not use personal mobile phones or electronic devices during work hours, unless on break or lunch
- Staff will only use school devices when contacting parents or pupils, recording or storing data, photos or information about pupils and families.
- Understand data protection laws around pupil and family data

Additional Responsibilities of Technical Staff

- Support PRUs and AP in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the AUP is being followed
- Report any E-Safety related issues that come to their attention to the E-Safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the Local Authority and others on e-safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the pupil AUP with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our community lies in effective education.

We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We believe that learning about E-Safety should be embedded across the curriculum and also taught in specific lessons in IT and PSHE.

We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP.

Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, with staff as appropriate, We have also prepared an E-Safety Information Pack for parents which will enable and empower them to have greater knowledge on how to promote safety in the digital world.

We request our parents to support the school in applying the E-Safety policy.

Managing and safeguarding IT Systems

The Hawkswood Group will ensure that access to the school IT system is as safe and secure as reasonably possible namely by ensuring that:

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for activity.
- Any administrator/master passwords for school IT systems are kept secure and available to at least two members of staff
- The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals
- We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on provided laptops.

Filtering Internet access

Web filtering of internet content is available from LGFL or our commissioned provider if requested. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around school as a reminder.

Access

The SLT decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive.

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in provision Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to provision systems is covered by specific agreements and is never allowed to unauthorised third party users.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the IT systems or a provided laptop or device and that such activity can be monitored and checked .

All users of the IT or electronic equipment will abide by the relevant AUP at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the service will provide email accounts for those staff as needed. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only.

There are systems in place for storing relevant electronic communications which take place between provision and parents.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Staff use of personal web mail accounts by staff is not permitted.

Publishing content online

The Hawkswood Group is currently redeveloping its web site and maintains editorial responsibility to ensure that content is accurate and the quality of presentation is maintained.

The Hawkswood Group maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number. Published contact details for staff are school provided.

Online material published outside provision:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in provision

Material published by pupils and staff in a social context which is considered to bring the service into disrepute or considered harmful to, or harassment of another pupil or member of staff will be considered a breach of discipline and treated accordingly

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

Using mobile phones

We recognise that the multimedia and communication facilities provided by a mobile phone can provide beneficial opportunities for pupils. However their use in lesson time will only be with permission from the teacher.

Mobile phones or similar devices with communication facilities used for curriculum activities are set up appropriately for the activity. Pupils are taught to use them responsibly.

Where required for safety reason in off-site activities, a school mobile phone is provided for contact with pupils, parents or the unit. Staff should not use their personal mobile forms to contact pupils or students.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber bullying', will be considered a disciplinary matter.

Using other technologies

As an education service we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.

We will regularly review the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined in this document.

Protecting data and information

The Hawkswood Group operates within the GDPR Regulations. We recognise our obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties. .

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with encrypted USB memory sticks for carrying sensitive data
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data

Dealing with E-Safety incidents

All E-Safety incidents are recorded in the E-Safety Log (Appendix 1 attached) which is regularly reviewed.

Any incidents where pupils do not follow the AUP will be dealt with following normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious E-Safety incident, concerning pupils or staff, they will inform the E-Safety coordinator, their line manager or head teacher who will then respond in the most appropriate manner.

Instances of **cyber bullying** will be taken very seriously by the service and dealt with using the anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the network, or create an information security risk, will be referred to the school's E-Safety coordinator and technical support. Appropriate advice will be sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The unit will decide if parents need to be informed if there is a risk that pupil data has been lost.

The Hawkswood Group reserve the right to monitor and search any technology equipment on the premises, including personal equipment, when a breach of this policy is suspected.

Annex 3 attached outlines behaviours which are deemed as inappropriate/unacceptable.

Dealing with complaints and breaches of conduct by pupils/staff:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies
- Annex 3 outlines

APPENDIX 1

PRU Staff /Volunteer Digital Acceptable Use Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the E Safety Co-ordinator.

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use school provided devices in school and will ensure where appropriate that they are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school IT systems.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- 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 not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school 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 E Safety Policy . Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and understand that I should only be using school owned devices when carrying out communications related to the school.

I confirm that I have received a copy of the PRU E Safety Policy and have made myselfaware of the contents within.

Staff / Volunteer Name (PRINT) _____

Signed _____

Date _____

Appendix 2

E-SAFETY RECORD FORM

Child's Name:	Class:	DOB:	Gender:

Date:	Time:	Place:	Name of person completing this form (please print):

Nature of Concern/Conversation (continue on a separate sheet if necessary) If relevant, please give name of any inappropriate web site accessed:

Name of person you reported your concerns to Date reported

Action to be taken / recommendations from the designated member of staff
Signed: Position:

Return the completed form to the Designated member of staff ASAP

Appendix 3

The following activities constitute behavior which we would always consider unacceptable (and possible illegal) :

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using facility or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988

The following activities would normally be unacceptable; however in some circumstances they may be allowed e.g. as part of planned curriculum activity or as system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another persona to log in using your account
- accessing unit IT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else