PROSPECT HOUSE

SCHOOL

DIGITAL USAGE POLICY

(INC E-SAFETY0 (305)

SEPTEMBER 2021

(text marked in blue refers to the Data Protection Policy or to data protection considerations)

DIGITAL USAGE POLICY

1. INTRODUCTION

Within the school, digital technology is integral and ubiquitous to the educational process as well as in the administration of Prospect House School. It is through this culture of exploring digital technologies that the curriculum is enhanced and the business workflows of the school is improved. The requirement to ensure that children and staff are able to use digital technologies safely and responsibly is addressed in this policy.

1.1. Scope

1.1.1 This policy covers the acceptable usage of digital technologies for all pupils (including those in the EYFS) and staff of the school. It applies to all members of the school community (including directors, teaching staff, support staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the school ICT systems both in and out of school.

1.1.2 The school will deal with any E-safety incidents in accordance with the procedures outlined in both this policy and associated school policies, such as the Safeguarding, Behaviour and Anti-bullying policies. Where necessary or appropriate, the school will also inform parents of any incidents of unacceptable or inappropriate use of technology that takes place out of school.

1.1.3 The school will deal with any data protection breaches in accordance with the procedures outlined in the Data Protection policy, as informed (where the breach involves digital technology) by this policy.

1.1.4 The term **'digital'** applies to all forms of technology and communications apparatus such as:

a) Computers

b) Laptops

c) Mobile devices

d) Reprographics

e) Video conferencing units

f) Cameras

g) Programmable toys

h) Software

i) Internet, Intranet, Extranet, Cloud resources

j) Email

k) Apps

l) All forms of social media/networking sites.

m) Internet of Things enabled device

1.2. Risks

1.2.1. The use of digital technology can put children and staff at risk both in and out of school. Annex D to 'Keeping Children Safe in Education' (September 2021)

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

categorises the main risks as:

- content: being exposed to illegal, inappropriate or harmful material; e.g. pornography, fake news, hate speech, racist or radical and extremist views

- contact: being subjected to harmful online interaction with other users e.g. adults posing as children or young people (grooming)

- conduct: personal online behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit images, or online bullying.

1.2.2. Adults are at similar risk to those for children.

1.2.3. Staff must also understand how to keep data safe by following the Data Protection Policy and must also be aware of and sensitive to the prevalence of phishing and malware websites and e-mails as well as their obligations and rights under the Data Protection Act 2018.

1.3. Aims

This policy aims to ensure that:

a) The school follows the statutory guidance on online safety in Keeping Children Safe in Education (September 2021) and other relevant guidance (see Paragraph 14).

b) To create a culture that incorporates the principles of online safety across all elements of school life

c) The school provides clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy

d) All staff and pupils, both in and out of school, are responsible users of technology for educational, personal and recreational use and benefit from its use

e) Pupils and staff are as clear about what is expected of them online as offline

f) Pupils are protected from potential risks in their use of technology and are educated to understand the risks posed by the Internet and social media to bully, groom, abuse or radicalise other people, especially children and young people

g) The school provides clear guidance on the use of technology in the classroom and beyond for all users, particularly staff and pupils, specifying where appropriate permissions/restrictions and sanctions for misuse

h) Staff and pupils are aware of their responsibilities with regard to this policy

i) The school's ICT systems are protected from accidental or deliberate misuse that could put the security of the systems at risk

j) The technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues are fit for purpose and robust

k) The school adheres to data protection requirements (please refer to the Data Protection Policy)

l) Reporting mechanisms are available for all users to report issues and concerns to the school, details as to how they are to be managed and/or escalated and how these link with other safeguarding procedures

m) The school informs, communicates with and provides guidance to parents/carers about use of digital technology in the children's education and online safety.

2. ROLES AND RESPONSIBILITIES

2.1. Head

2.1.1. The Head, has overall responsibility for E-safety within the school. The day-to-day management of this will be delegated to the E-safety officer (Dee Edwards). The E-safety officer in the school is the member of staff with responsibility for computing. The Data Protection Policy sets out responsibilities regarding data protection.

2.1.2. The Head of the school is responsible for ensuring that the school has effective policies and procedures in place and as such will ensure that:

a) this policy is reviewed at least annually

b) the policy is up to date, covers all aspects of current technology use, and that the policy is effective in managing any E-safety incidents

c) E-safety and data protection training throughout the school is planned, up to date and appropriate for the recipients, e.g. pupils, all staff, senior leadership team and parents

d) all E-safety and data protection incidents are reported promptly and dealt with appropriately

e) the E-safety officer and other relevant staff receive suitable training to enable them to carry out their E-safety roles and train other colleagues, as relevant

f) there is full awareness of the safeguarding procedures to be followed in the event of an E-safety incident

g) there is a full awareness of the data protection procedures to be followed in the event of a data breach (see the Data Protection Policy)

h) she or he keeps up-to-date with the latest advice and guidance on the subject of E-safety and data protection.

2.2. Governors

2.2.1 The governors will ensure that the school

a) keeps up to date with emerging risks and threats through technology use

b) ensures that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach

c) receives regular updates from the Head in regard to training, identified risks and any incidents

d) ensures children are taught about safeguarding, including online safety, through the Computing curriculum and PSHCE

e) ensures that data protection compliance training for staff is integrated, aligned and considered as part of staff core training and that additional data protection awareness and training is otherwise sufficient to ensure staff are live to the need to protect personal data processed by the school.

2.2.2. The Head will have overall responsibility for the E-safety and data protection at the school.

2.3. E-safety officer (computing coordinator at the school)

2.3.1 The school's Head of computing is responsible for the day to day duties of managing E-safety. The E-safety officer will be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from

a) sharing of personal data

b) access to illegal/inappropriate materials

c) potential for actual incidents of grooming

d) online bullying.

2.3.2 The E-safety officer will

a) report all E-safety incidents to the Head immediately

b) keep up to date with the latest risks to children whilst using technology

c) be familiar with the latest research and available resources for school and home use

d) review this policy regularly and bring to the attention of the head any matters that might make an amendment desirable

e) advise the Head on all E-safety matters

f) engage with and educate parents and the school community on E-safety matters at school and/or within the home

g) liaise with Technical Support and other agencies as required

h) retain responsibility for the E-safety incident log and report all incidents to the head

i) ensure staff know what to report and that all safeguarding incidents are reported to the DSL as outlined in the Safeguarding Policy

j) through liaison with Technical Support, ensure any technical E-safety measures in school (e.g. internet filtering software) are fit for purpose

k) be aware of any reporting function with technical E-safety measures, e.g. internet filtering reporting function, liaising with the Head to decide on what reports may be appropriate for viewing

l) approve or disapprove YouTube videos on the Google Apps for education platform.

2.4. Technical support staff

2.4.1. The Technical Services team are responsible for:

a) keeping up to date with emerging risks and threats through technology use

b) liaison with the Head of the school and the Head of computing in regard to training, identified risks and any incidents

c) liaison with the school data compliance officers in regard to training, identified risks and any data breach incidents

d) ensuring the IT technical infrastructure is secure, which will include as a minimum:

(i) anti-virus is fit-for-purpose, up to date and applied to all capable devices

(ii) system updates are regularly monitored and devices updated as appropriate

(iii) any E-safety technical solutions such as internet filtering are operating correctly

(iv) filtering levels are applied appropriately and according to the age of the user

(v) categories of use are discussed and agreed with the E-safety officer and Head

(vi) passwords are applied correctly to all users regardless of age - See section on password policy (paragraph 6 below)

(vii) ensure that the use of USB memory sticks are limited only to those who have been given explicit permission to use them and where these are used, they always sanitised for viruses or malware before being connected to any school network

(viii) ensure that the school’s approach to the retention of data is followed

e) ensuring that all devices taken off site are sufficiently encrypted, and password protected.

f) setting an example and being a model digital citizen to all pupils, staff and parents engaging where appropriate in conversation and advice on E-safety and digital usage.

2.5. All staff (including support staff)

2.5.1. Members of staff must ensure that:

a) All details within this policy are understood. If anything is not understood it must be brought to the attention of the Head

b) He or she has an up-to-date awareness of E-safety and data protection matters and of the school online safety policy and practices

c) He or she has read and understood the staff and pupil acceptable usage policies (for pupils, see Appendix I; for staff, see Appendix II for pupils)

d) He or she reports any suspected misuse, problem or E-safety incident to the E-safety officer and Designated Safeguarding Lead (DSL) immediately

e) Any digital communications with pupils (email, cloud platforms) are on a professional level and only carried out using official school systems, adhering to this policy

f) He or she embeds safe and responsible usage of digital technology in all aspects of the curriculum and other school activities

g) He or she ensures pupils follow the pupils' acceptable usage policy and understand the tenets of pupils' appropriate digital usage as set out in section 2.6 below

h) He or she acts as good role models for the pupils in their use of digital technology

i) That any data breach is immediately reported in accordance with the Data Protection Policy

j) Each understands the reporting flowcharts contained within this policy.

2.6. All pupils

2.6.1. All staff are responsible for making pupils aware of the following aspects of digital usage:

a) to appreciate online safety issues and to act responsibly in their use of digital technology

b) to use school digital equipment in accordance with the acceptable usage policy for pupils

c) to understand the importance of reporting abuse, misuse or access to inappropriate materials and to know how to report such to any member of the teaching staff

d) to have a good understanding of research skills and the need to avoid plagiarism and uphold the copyright of others

e) to understand the school's policies on the use of mobile devices

f) to understand the school's policies on the taking and use of images

g) to understand the school's policies on online bullying

h) to carry the same level of understanding and follow these policies outside school.

2.6.2 The boundaries of use of ICT equipment and services in this school are set out in the Pupils' Acceptable Use Policy (see Appendix I to this policy). Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the school's Behaviour Policy.

2.7. Parents and carers

2.7.1 Parents play the most important role in the development of their children. The school will therefore do all that it reasonably can to ensure that parents have the skills and knowledge they need to ensure the E-safety of children outside the school environment. Through parents' evenings, school circulars and newsletters the school will keep parents up to date with new and emerging E-safety risks and will involve parents in strategies to ensure that pupils are protected.

2.7.2 Parents will be encouraged to support the schools by

a) promoting good online safety practice

b) following the guidelines on safe and appropriate use of technology

c) accessing the secure parents' section of the school website as instructed by the school

d) supporting and endorsing the guidance set out in the pupils' acceptable usage policy.

3. EDUCATION STRATEGIES

Whilst the school uses technical procedures for the control of and monitoring of internet activity, it is the marriage of these protocols with the protocols on behaviour that create the most secure environment.

Children, including those in the EYFS, will be taught to recognise and avoid online safety risks and to behave online in an appropriate manner. This will largely take place through the computing and PSCHE curriculum but will also be manifest in the general ethos of the school towards online behaviour.

Staff will be kept up to date with the latest legislation and advice from the DfE and from other organisations such as CEOP (Child Exploitation & Online Protection) and the NSPCC.

Parents will receive help and advice from the school to create safe online environments at home and outside of school.

Education is therefore an essential part of the school's digital safety provision.

3.1. Staff

3.1.1 It is essential that staff receive E-safety and data protection training and understand the above responsibilities. Training will be offered as follows:

a) At least one member of staff across the school will be trained to the CEOP Ambassador level so that up-to-date E-safety training can be disseminated to all staff. This is Mr Kevin Chung.

b) All new staff will receive E-safety and data protection training as part of their induction programme, ensuring that they understand the acceptable usage policy and their responsibility to follow the reporting procedure

c) Any new E-safety issues will be brought to the attention of staff at staff meetings

d) All staff will receive refresher training sessions once a year.

e) In addition staff will receive regular updates and training in staff meetings about digital usage.

3.2. Pupils

3.2.1 E-safety is embedded into the school's curriculum; pupils will be given the appropriate advice and guidance by staff

3.2.2. All pupils will be fully aware of how they can report areas of concern whilst at school or outside school

3.2.3. A separate computing policy for the school details methodology and topics for the teaching of computing and digital literacy

3.2.4. Pupils will be taught the importance of safe and responsible technology usage as part of their computing lessons and through the PSHCE curriculum; this will include using a selection of E-safety books and resources, including those developed by CEOP. A detailed outline of the topics covered within each year group can be found in the Computing and PSCHE Schemes of Work for the school. At all times due consideration is given to the age and level of understanding of the pupils

3.2.5 From September 2020, Relationships Education will be compulsory for all primary-aged pupils. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. This will complement the existing computing and PSHCE curriculum.

3.3. Parents

3.3.1. At the beginning of each academic year, parents are invited to a curriculum evening, which will usually include items on E-safety and at parents' evenings, and the computing teacher will be available to talk to parents about the E-safety teaching which takes place in class. Parents have the opportunity to seek advice from the school's technical services team, who can advise on home strategies for E-safety at the start of each academic year

3.3.2. The school's website has a link to http://parentinfo.org, which is a free service for schools and parents that provides expert information to help children stay safe online. Through this service, parents are able to look up information and obtain the best security practice information on websites and apps that are popular with children.

4. PROCEDURES

4.1. The technology

4.1.1. The school is committed to an on-going programme of replacement and enhancement of ICT equipment and software. New computers are bought as necessary each academic year either as replacements or as additional resources and the school is therefore continuously improving its resources. All classrooms have an interactive whiteboard and computer

4.1.2. Computing departmental expenditure is monitored centrally by Dukes Education. New equipment is purchased on an 'as needed' basis and funding is generous

4.1.3. Staff can request help/support/advice about software from the Head of computing who will negotiate and arrange the purchase and installation of any necessary software within the limitations of the annually-approved budget. Members of staff should never place such a purchase order themselves. This is because all suppliers of software are vetted: where the processing of personal data is concerned, a data sharing agreement will be formed between the supplier and school, while software security (e.g. propensity to viruses or malware) is also assessed

4.1.4. The school uses a range of digital devices. In order to safeguard the pupils and in order to prevent loss of personal data the technology described in paragraphs 4.2 et seq below is employed.

4.2. Filtering

4.2.1. The school uses a hardware firewall with a content filtering service that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. What is considered to be appropriate and inappropriate is determined by the age of the user and is reviewed in line with this policy or in response to an incident. The Head of Computing is responsible for ensuring that the filtering is appropriate and that any issues are brought to the immediate attention of the Head

4.2.2. Email Filtering for pupils

4.2.2.1 The school uses G-Suite for Education as an email server for pupils. This type of email server prevents any unauthorised senders sending emails to school pupils. Pupils will also not be authorised to send emails to recipients outside the defined 'safe list', which include domains of the other schools and certain educational bodies

4.2.3. Encryption

4.2.3.1. All school devices that are taken off site and hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data is ever allowed to leave the school on an unencrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) must be addressed in accordance with the Data Protection Policy

4.2.4. Google Safe Search and YouTube Restricted Mode

4.2.4.1. All devices within the school are programmed to route Google searches only through the Google safe search site, which displays only safe search results. When accessing the YouTube video sharing site, all pupil devices within the school are programmed into 'restricted YouTube' mode, which restricts videos and audio clips to those that are appropriate

4.3. Passwords

4.3.1. The correct use of passwords is fundamental to proper data usage. See Paragraph 6 below for more detailed information on passwords
4.3.2. All devices within the school are to be considered public devices and passwords must not be saved on school devices.

4.4. Anti-virus

4.4.1. All school devices have anti-virus software where this is feasible. This software is updated at least weekly for new virus definitions. IT Support is responsible for ensuring this task is carried out and will report to the head if there are any concerns. All USB peripherals such as keydrives must be scanned for viruses before use. (See also BYOD paragraph 8.)

4.4.2. Viruses are also scanned on the firewall level, so viruses are automatically blocked and monitored. This guards against such viruses from infecting computers behind the firewall. (This therefore applies to all devices except those that connect via the mobile network.)

4.5. Emails

4.5.1. The school's email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Staff must understand that the emails they send and receive are official records that can be disclosed to relevant parents, staff, other third parties or to the Information Commissioner's Office (ICO) if a subject access request (SAR) is made. Staff are required never to use email communication casually

4.5.2. The school has an email component linked to the internet server. Email addresses are created using the model: firstname.lastname@apps.prospecths.org.uk with the exception of the Head whose e-mail is initials.lastname@prospecths.org.uk

4.5.3. Access is as follows:

a) Pupils have access to the email messaging service via their G-Suite account, allowing them to email a restricted number of addresses specifically permitted by the ICT staff, these being primarily school addresses and specified other addresses that have been approved
b) Members of staff may send and receive emails externally but not to parents to whom messages must be sent only through the school office
c) Staff are able to access their school emails from home and will need to follow the procedure on how this may be achieved via the webmail link on the school's website.

4.5.4. Staff should use their school email address for correspondence of a professional nature. It is unacceptable to use personal email addresses for school or professional communication. Similarly, except with the consent of the Head it is unacceptable for any, member of staff to forward data related to the schools and/or to children to any email external addresses including their own personal email. For example, staff must not forward a child's report from his/her school email account to his/her personal account.

4.5.5. All emails from the school addressed or copied to an e-address external must by law show at the foot of the email the school's (or, where relevant for central staff) statutory footer, and it is good practice to show the school's telephone number, thus:

Prospect House School – Putney
(Registered in England No.2274105)
75 Putney Hill, London SW15 3NT
www.prospecths.org.uk/privacy/
www.prospecths.org.uk
Tel: 020 8780 0456

4.5.6. If the relevant footer is appropriately displayed earlier in an e-trail of emails such that, by scrolling down, it can easily be seen, then it need not be repeated in later emails where these are within the same linked trail.

4.5.7. Staff must not engage in any email correspondence which could be viewed as offensive or makes unsubstantiated claims or gossip about other staff, parents or pupils. Staff are permitted to check their personal email accounts but should do so at lunch and break time only; access at other points during the working day should be avoided. Staff should be aware that, if the Head believes that traffic generated by or sent to a member of staff may have been inappropriate or in contravention of any other school policies, the school reserves the right without notice to inspect and review email traffic that has passed through or is resident upon the schools' system. Staff must also be careful to avoid any email traffic being displayed inadvertently on a whiteboard or a computer screen such that it could be overlooked by a child or other member of staff to whom the data on display is not relevant and may be inappropriate.

4.5.8. Staff must be aware that some email client programs, such as Microsoft Outlook, give alerts when emails are received, so staff should avoid typing in sensitive material, e.g. 'Susie leaving at end of term' in the subject line. These alerts can be turned off within 'Preferences' or via a request to the school's Technical Support team via a KevKall. Emails must be checked at least once in the morning, at lunchtime and before leaving at the end of the school day. Please refer to the Acceptable Usage Policy – Staff.

4.6. Use of the internet

4.6.1 Staff should use the internet at work primarily for work-related tasks; any personal usage should be sparse and in rest breaks only, such that it does not interfere with the performance of the member of staff's duties or with the normal operation of the school internet (e.g. downloading large files could slow the internet for other users). Staff must not use work devices to view or distribute inappropriate content. In particular, staff must not:

a) take part in internet activities which could bring the school into disrepute,

b) create or transmit material which might be defamatory for the school or which could create an unwanted liability for the school,

c) view, download, create or distribute any inappropriate content. Inappropriate content includes pornography, racial or religious slurs, content relating to illegal drug use, gambling or which facilitates or promotes criminality. Inappropriate content is also any content which could lead to a claim of unlawful discrimination

d) use any programmes or software to bypass the school security systems.

4.6.2 The above rules on use of the internet also apply to browsing the internet on a device owned by the school even when not at work.

4.6.3 The school reserves the right to monitor and review the internet usage of any member of staff at work or on a school owned device and to take disciplinary action (up to an including summary dismissal) for use which contravenes this policy.

4.7. Contact with Parents

4.7.1. Emails to and from parents: staff must forward all email communication with parents to the school's office. An intended outbound email can then be sent on from the school's general office email address, info@prospecths.org.uk address. **There can be no exceptions to this rule.** Heads are given the facility on their desktops to respond to email traffic from their school's 'info' address and this address is always to be preferred.

4.7.2. Emails from parents must be responded to before the close of the day, although in the case of a complex enquiry initially it is adequate to state something like 'Thank you for your email. I am looking into this and will respond by…' stating a date by which the school will respond in substantive terms. Such complex emails must always be brought to the attention of the head, even if the office or another member of staff will resolve the query.

4.8. Contact with external processors when personal data is shared

4.8.1. Emails sent from the school mail services such as Office 365 and Google Mail are naturally encrypted during transit so that they cannot be intercepted. When sending emails with personal data to external processors such as the NCTL or the LA, the school office may consider further encryption whereby those emails can only be read by those intended recipients whereby those recipients will require a separate key to open the email.

4.9. Phishing and ransomware

4.9.1. The school uses Apple Mail, Google Mail and Microsoft 365 servers. This mostly prevents infected email being sent from or being received by the school. "Infected" is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data or spam email such as a phishing message.

4.9.2. Ransomware is a type of computer virus that gives criminals the ability to lock files on a computer that the criminals have infected – the screen then displays a pop-up window informing the user that the computer will not be unlocked until a sum of money is paid. An additional twist is that an accusation of illegal activity or a pornographic image often appears on the locked screen, making it more difficult and embarrassing for users with infected machines to seek help from anybody else: many users simply resort to paying the ransom sum demanded by the criminals to supply an 'unlock' code. The technical procedures detailed below put in place counter-measures against ransomware. However, alongside creating technical policies and installing machines to control what to let in or out of the school, we also need to be extremely vigilant in what we open and send on in emails as well as taking great care in choosing websites we browse. It is the marriage of machine protocols and of user behaviour that creates the best and most effective anti-virus strategy. Staff are reminded to digest and follow the rules below:

a) Be alert to email traffic, whoever the sender at first glance may appear to be. Infectious viruses can arrive in the guise of what purports to be an email from a colleague. If you receive an email with an attachment or containing a link, even if it seems to be from a colleague, always question why he or she has sent you that email. Ask yourself whether the email raises any reason for suspicion. If you harbour any suspicions about the email, please do call the colleague who appears to have sent it to check that he or she was indeed the sender. Staff with good IT knowledge can also inspect such emails via "view source" or similar within each email client and this will often include the true origin of an email, including an extension associated with some implausible name and/or improbable country.

b) Never log in to external websites (unless it is Google/G suite or are under the guidance of your school's Head of computing or the IT team). Opening any attachment that redirects the user to a website to login, must always be done under specialist supervision from the IT team. It is highly unlikely that a colleague will send an attachment that directs a user to a page to log in. Users should already be logged in if they are receiving emails and must never log in again. This applies no matter how convincing the address bar and web page looks.

c) Even when it is Google/G Suite, check the Google address. The user should only be prompted to log in to a legitimate service, such as when opening Google Drive or G Suite for education. Users should always check the address bar to verify the web address.

d) Never enable macros on documents or files sent from an external address. If, on opening a document any request to enable "Macros" must be declined. Many ransomware viruses are embedded in Microsoft Office documents, which trick the user to running a malware macro that then infects the computer.

e) If ever a user is uncertain,, log a request for technical support through the technical support website (KevKall).

4.10. Archival and the retention of emails

4.10.1. The retention period of pupil, parent and staff data is covered within the Data Protection Policy. Emails that are stored on school systems are backed up and archived according to this policy which means that emails are (so far as practicable) kept for 50 years.

4.11. Children's email accounts

4.11.1. Children are given access to a school email account (subject to approval by the school), following on from a module of work on internet and email safety. The format of this account is to be firstname.surname@apps.prospecths.org.uk with an alphanumeric password at least eight characters long. Children can access their email accounts at both home and school and proper use of this forms the basis of teaching good electronic communication skills.

4.12. Contact with children

4.12.1. The school email system allows children to communicate with staff at any time including out of school hours. This allows the children to submit work and request help but must not be used for any personal communication with the children. Staff are also under no obligation to respond to an email from a pupil arriving outside normal school hours.

4.12.2. In order to maintain a high level of professional communication between staff and children, the school reserves the right to monitor email communications and postings on internal school sites.

4.13. Photographs and video

4.13.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

4.13.2. When using digital images staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. social networking sites.

4.13.3. Staff and volunteers are allowed to take digital/video images to support educational, promotional or marketing purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken only on school equipment: the personal equipment of staff should not be used for such purposes wherever possible, unless the Head has given specific prior permission.

4.13.4. The school's privacy notices for parents indicate that photographs of their child(ren) may be used in school publications, on the school website or in other materials created or promoted by the schools in the public domain.

4.13.5. For any external use of digital images:

a) if the pupil is named, the school does not publish a photograph

b) if a photograph is used, the school avoids captioning the photo with the pupil’s name

c) when showcasing examples of pupils’ work, only first names are used

d) if showcasing digital video work to an external audience, care is taken to ensure that pupils are not referred to by name on the video and that pupils’ full names are not given in the credits at the end of the film

e) only images of pupils in suitable dress are used.

4.14. Social networking by staff

4.14.1. There are many social networking services available and the schools are fully supportive of social networking as a tool to engage and collaborate with the parents of current and prospective pupils. The following social media services are permitted for use within the school and have been appropriately risk assessed. Should staff wish to use other social media, permission must first be sought via the E-safety officer who will consult the head for a decision to be made. Any new service will be risk assessed before use is permitted.

a) Blogging – used by authorised staff and pupils in school office and PE staff

b) Twitter – used by the school as a broadcast service (see below)

c) Facebook – used by the school's office

d) Instagram – used by authorised staff and the school office as a broadcast service.

4.14.2. A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

4.14.3. In addition, the following is to be strictly adhered to:

4.14.4. There is to be no identification of pupils by name

a) Where services are "comment enabled", comments are to be set to "moderated"

b) All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

4.14.5. Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

4.14.6. Further guidance for staff on social networking use is contained in the staff code of conduct within the Safeguarding Policy.

4.15. Digital usage of personal data

4.15.1. The Data Protection Act 2018 provides considerable protection of pupils' personal data, and the UK data protection watchdog, the Information Commissioner's Office (ICO), has fined educational establishments and individual teachers found to be failing in the duty to keep such data secure. The following guidelines will assist staff in processing personal data.

4.15.2. Data which comprises photos of children must only be used at school or on a school device. The school encourages staff to take photos and videos of children at work and play, as these are important aspects of school life to record and are welcomed by children and parents alike. However, basic disciplines must be observed. It is acceptable only to take images and video of children in the classroom on a school device.

4.15.3. The use of personal data held within the school should not be abused. Such use must be proper, and further guidance on lawful use of data in education is available from the guidance section of the Information Commissioner's website at https://ico.org.uk/for-organisations/guidance-index/ In brief, under the DPA 2018, the school and its staff must:

a) only collect information that is needed for a specific lawful purpose

b) keep it secure

c) ensure it is relevant and up-to-date

d) only hold as much as is needed, and only for as long as it is needed

e) allow the subject of the information to see it on request

f) only hold onto the data for as long as it is lawfully required

g) allow the subject of the information to erase some or all data concerning the subject if this does not also hinder safeguarding aspects.

4.15.4. Education and the school's Head take the security of pupils' personal data extremely seriously. Data pertaining to children, such as academic records, examination and test data etc, should **never** be taken off school premises unless specific written authorisation has been obtained from the Head of the school or, in her or his absence, from the Head of computing. This rule applies not only to laptops but also to disks, USB memory sticks, mobile phones, iPads, mp3 devices or any other electronic device upon which data may be stored. If such authorisation has been obtained, then even with this authority the member of staff seeking to take data off site must nonetheless liaise with the Head of computing at the school, or the IT technical staff, to ensure proper data security encryption or file protection is in place. Permission for third-party access to the school's Management Information System can only be granted once written approval has been given by the school's Head.

4.15.5. If pupils' personal data is required by a teacher working elsewhere, for example, for the analysis of work or the writing of reports, then remote access is granted via the Google G-Suite ecosystem of applications such as Google Drive, Google Docs and Google Sheets. Staff must only use Google G-Suite through an Internet browser and must not download any content from that platform onto their personal device. The only exceptions to this rule are certain school staff (bursary and IT technical staff), the Head, Deputy head, Head of Lower School and the Head of computing, all of whom use computers that are school property and each of whom must be satisfied about the installation and activation of full disk encryption (FDE) on his or her laptop so as to offer greater security to any data held upon them or, in the alternative, that the laptop is protected by a file security program such as FileVault™ or similar, or both. For any such member of staff, when travelling with such a device (typically a laptop), it is essential, if FDE is to be an effective security measure, that the machine is also fitted with an effective screensaver password and also that it is on each occasion shut down before transit.

4.15.6. It follows from the two paragraphs above that, save for the exceptions noted therein, no personal data should ever be in transit on any IT device outside of the school. Failure to comply with this aspect of this policy will be regarded as a very serious disciplinary breach and could result in a fine by the ICO on the individual member of staff.

4.15.7. If a member of staff authorised so to do is working on such data remotely held in a semi-public place, eg upon a train or in a café, he or she must, in addition to ensuring that inappropriate eyes may not snoop, shut down the device whenever it is not fully supervised. Use of laptops etc. in such surroundings is always risky and should where possible be avoided.

4.15.8. When a teacher leaves the school's employ, should there be any personal pupil data inadvertently remaining off-site on a personal system then this must immediately be reported and also all instances must be deleted. Any devices that belong to the school, such as laptops, iPads, USB memory sticks, or hard-drives, must be returned to the school's office.

4.15.9. The school uses cloud services for teaching and learning (setting and marking homework), communication and curriculum management.

4.15.10. In accordance with the DfE's guidelines on cloud computing and the GDPR, the following services have been chosen by the school. These organisations have participated in the DfE's self- certification scheme.

a) G-Suite for Education

- Google Classroom
- Google Drive
- Google Calendar

b) Microsoft 365

- Microsoft One Drive
- Microsoft Office Suite

4.15.11 All external educational suppliers which process pupil data on the school's behalf have been audited for their DPA 2018 compliancy. This process is conducted using the GDPRiS platform whereby suppliers are registered with GDPRiS and have shared with it their data sharing agreement.

4.15.12 As above, any of these suppliers which store data outside of the EEA have been vetted so that they appear on the Privacy Shield, which is a mechanism for U.S.- and EEA- -based companies to comply with cross-border data protection requirements.

4.15.13 For more information on the DPA 2018 and data protection, please refer to the Data Protection Policy.

2. INCIDENTS

5.1 E-safety incident

5.1.1 It is expected that all members of the school community will be responsible users of ICT who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, deliberate misuse. An online safety incident is defined as a violation of the Staff Acceptable Usage Policy (set out in Appendix II below), or of the Pupils' Acceptable Usage Policy (set out in Appendix I below), or a safeguarding incident involving technology. If a member of staff suspects that misuse might have taken place, that member of staff should follow the following procedures in reporting the incident.

5.1.2. Children should be regularly reminded to report anything they feel unhappy with and staff must act upon this according to the online safety procedures.

5.1.3. In the event of an accidental online safety incident, e.g. a child or staff member inadvertently accessing inappropriate material, the school's E-safety officer must be informed for an investigation to be carried out and a KevKall ticket completed.

5.1.4. Where cyberbullying is identified, the matter will be reported immediately to the Head and the E-safety officer.

5.1.5. Where the matter is not bullying but is a child protection issue, reporting processes as laid out in the Safeguarding Policy will be followed. The initial step is to immediately report the matter to the DSL (designated safeguarding lead).

5.1.6. If a member of staff suspects that misuse might have taken place, but that the misuse is seemingly a minor infringement and is not illegal e.g. a staff member using ICT for personal use or a child using another child's login details, these steps should be followed:

a) Staff must use KevKall (https:kevkall.houseschools.com) and select the help topic title "Report an E-safety incident" to report incidents

b) The E-safety officer must be informed

c) The E-safety officer will need to judge whether this concern will require an investigation and will report the incident to the Head

d) If the result of the investigation has substance, then appropriate action will be required and could include internal response or disciplinary procedures

e) if the incident gives rise to any safeguarding concern, this must be reported immediately to the DSL

5.1.7. In the event of suspicion of deliberate misuse and the incident is serious e.g. a member of staff looking at websites that incite racial hatred or a child has uploaded inappropriate images of him/herself, the following procedure should be followed:

a) The device should be locked

b) No images or content should be forwarded nor should the devices be searched for further content

c) The incident must be reported to the Head and E-safety officer immediately

d) The E-safety officer will liaise with he Technical Support Team immediately so that URLs are closely monitored and recorded (to provide further protection)

e) Isolate the computer in question as best you can. Any change to its state may hinder an investigation

f) Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation

g) If the content being reviewed includes images of child abuse then the monitoring should be halted and the DSL will consider the situation in accordance with the Safeguarding Policy. Other instances would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child or adult material which potentially breaches the obscene publications legislation
- criminally racist material
- other criminal conduct, activity or materials
- material related to radicalisation.

6. PASSWORDS

The school treats data security very seriously, especially as its digital services are available outside the physical confines of the schools. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of the school's data resources. All users, including contractors and vendors with access to the school's systems, are responsible for taking the appropriate steps outlined below to select and secure their individual passwords.

6.1 Purpose

6.1.1 The purpose of this password policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

6.2 Scope

6.2.1. The scope of this password policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at the school facility or any cloud-based service that the school subscribes to, that has access to the school's network or that stores any non-public school information.

6.3 Where this policy applies

6.3.1. This policy applies to the following but is not limited to these services:

a) MacOS Network account (school login)
b) Wifi networks
c) School email accounts
d) School G-Suite accounts
e) iSams
f) School websites
g) Policies and Knowledge Bank Matrices
h) School intranet
i) Tapestry
j) CPOMS
k) School online galleries
l) Online learning services including but not limited to:

- Mathletics
- Atom Learning
- IXL

6.4 Password change frequency

6.4.1. All system-level passwords (e.g. root, system administrator, local administrator etc) will be changed on at least a yearly basis by the IT team.

6.4.2. The passwords to all staff accounts should be changed at least on a yearly basis and at any point promptly if the user should come to believe his or her password has been compromised.

6.5 Secure passwords

6.5.1. All system-level passwords (e.g. root, system administrator, local administrator etc) must be strong rather than weak, please refer to guidelines below.

6.5.2. Similarly all staff accounts should also be strong

6.5.3. All users should be aware of how to select strong passwords.

6.5.4. Construction guidelines for strong passwords

a) Contains at least three of the five following character classes:
b) Lower case characters
c) UPPER CASE CHARACTERS
d) Numbers
e) Punctuation
f) "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
g) Contains at least 8 characters

6.5.5. Conversely, weak passwords have the following characteristics:

a) The password contains less than 8 characters
b) The password is a word found in the dictionary (Foreign or English) - even if it is alpha-numeric!

c) The password is a common usage word such as:

d) Names of family, pets, friends, co-workers, fantasy characters etc

e) Birthdays and other personal information such as addresses and phone numbers

f) Word, number patterns or palindromes such as aabb, qwerty, 123321 etc

g) Any of the above preceded or followed with a digit (e.g. kevinchung1, daddychung1982, prospectschool2014 etc)

6.5.6. Password protection: how to help yourself

a) Always use different passwords for school accounts from other non-school access (e.g. personal email accounts, ISP etc)

b) Do not share school passwords with anyone

c) Passwords should never be written down or stored electronically without encryption (e.g. Do not write down a password on a sticky note and stick this to your computer!)

d) Do not reveal passwords in email or other electronic communications

e) Do not hint about the format of passwords

f) If someone should ask for help with a password, please refer them to this document

g) If compromise of an account or password is suspected, report the incident on the E-safety officer and KevKall it immediately.

7. Enforcement

7.1. It is very important this policy should be followed by staff carefully and diligently; departures from it will be investigated and may result in disciplinary action.

8. BRING YOUR OWN DEVICE (BYOD) - STAFF

8.1 Purpose

8.1.1. There is a 'laptop for teachers' scheme sponsored by the school being introduced in 2021-22 as part of the school's mobile device strategy.

8.1.2. There is no shortage of access to computers for staff on the school premises. These include, but are not limited to desktop computers in classrooms and in each staffroom. Access to digital devices is prioritised for pupils at all times.

8.1.3. The intent of this is to grant teachers, secretaries and support staff (the staff) the privilege of using personal devices such as laptops, smartphones, tablets (the personal device) of their choosing to complete school-related tasks such as teaching, communication and administration at the discretion of the Head on school property and by using the school's computer network (wireless or wired). For verification purposes when accessing sites such as CPOMS, iSAMs, and Google, personal smartphones may be used/visible in classrooms and other workspaces.

8.1.4. The school reserves the right to revoke this privilege if a member of staff does not abide by this policy when using a personal device on school property.

8.1.5. This policy is intended to provide staff an offering of internet bandwidth, access to the school's electronic resources and also to protect the integrity of the school's data and network infrastructure at the same time as conserving the human and time resources of the Technical Support team.

8.2. Use of personal devices

8.2.1. Violation of these rules and of course any criminal laws associated with electronic devices will result in appropriate disciplinary and/or legal action.

8.2.2. Staff use of a personal device on school premises is at the discretion of the Head and Head of computing and must be encrypted prior to its use for this purpose.

8.2.3. Access to the network for personal devices is provided over wifi whereby the wifi password is provided to the member of staff requesting it and it is granted on an individual basis.

8.2.4. When using a personal device on school premises, the member of staff must abide by the Digital Usage policy whether the device is connected to the school's wifi or connected to the member of staff's personal mobile data network. i.e. although the access to the world wide web is censored when using the school's wifi network, the member of staff must not break the acceptable usage policy (Appendix II) by browsing to unsolicited websites on his or her own personal mobile data network when on school premises.

8.2.5. Staff personal devices may not be used to establish an 'ad-hoc' or 'peer-to-peer' or 'personal hotspot' network whilst on school premises.

8.2.6. Staff use of a personal device on school premises is strictly for school work and should not be used for personal non-school related activities and must certainly not distract other colleagues in their school duties.

8.2.7. If staff take photographs of children on a personal device, no such photographs or video imagery must be kept on the staff's personal device. If needed to be kept they must be uploaded on to the school systems and then immediately deleted from the personal device. Digital images of children on personal devices must never be taken offsite.

8.2.8. Whilst technical support is provided for personal devices, it is only provided on a goodwill basis. There is no obligation on the part of the Technical Support team to fix, maintain or upgrade staff's personal devices. Staff should request technical support through the KevKall system but understand that a request of this nature will be marked as low priority.

8.2.9. Personal devices are brought on to school premises at the staff's own risk. The school will not take responsibility for any lost, stolen or broken personal devices while they are on or in transit to or from school premises.

8.2.10. The E-safety officer and the Head reserve the right to seize and examine a personal device if there is reasonable suspicion that school policies or criminal laws have been violated.

9. POLICY MONITORING

9.1. The implementation of this digital usage policy will be monitored by the E-safety officer at the school. It will be developed in light of its success, significant new developments in the use of the technologies, new threats to digital safety or incidents that have taken place.

9.2. Should online incidents take place, the school's DSL and the E-safety officer must always be informed.

10. LEGISLATION AND GUIDANCE

The following statutory and non-statutory guidance has been reflected in this policy.

- DfE statutory guidance - Keeping Children Safe in Education (September 2021)
- Teaching Online Safety in Schools (June 2019)
- Safeguarding Children and Protecting Professionals in Early Years Settings (February 2019) advice for managers and practitioners
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- UK Council for Child Internet Safety (UKCCIS)
- The Data Protection Act 2018
- the GDPR, the DPA and any relevant guidance from the Information Commissioner's Office (ICO)

11. Information and support

There is a wealth of information available to support schools and parents to keep children safe online. The following is not exhaustive but provides a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

https://www.nspcc.org.uk/onlinesafety
https://parentzone.org.uk/

APPENDIX I - ACCEPTABLE USAGE POLICY – PUPILS

(This Acceptable Usage Policy is printed, laminated and displayed in all classrooms in KS2.)

I promise to use the school ICT only for schoolwork that a teacher has asked me to do.

I promise not to look for or show other people things that may be upsetting.

I promise to show respect for the work that other people have done.

I will not use other people's work or pictures without permission to do so.

I will not damage the ICT equipment. If I accidentally damage something I will tell a teacher.

I will not share my password with anybody. If I forget my password I will let my teacher know.

I will not use other people's usernames or passwords.

I will not share personal information online with anyone.

I will not download anything from the internet unless a teacher has asked me to.

I will let a teacher know if anybody asks me for personal information.

I will let a teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will be respectful to everybody online.

I will treat everybody the way that I want to be treated.

I understand that some people on the internet are not who they say they are, and some people can be nasty. I will tell a teacher if I am ever concerned in school, or tell my parents if I am at home.

I understand if I break the rules in this acceptable usage policy there will be consequences and my parents will be told.

APPENDIX II - ACCEPTABLE USAGE POLICY – STAFF

(This Acceptable Usage Policy is laminated, printed and displayed in all staff common areas.)

Internet access – Staff must not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: child abuse; pornography; discrimination of any kind; the promotion of racial or religious hatred; the promotion of illegal acts; statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activities; contain threatening behaviour, including promotion of physical violence or mental harm; any information which breaches the integrity of the ethos of the school or brings the school into disrepute or any other information which may be illegal or offensive.

Inadvertent Internet access must be treated as an E-safety incident, reported to the E-safety officer and a Kevkall incident completed.

Social networking – This is allowed in school in accordance with the E-safety policy only and as outlined in the Staff Code of Conduct within the Safeguarding Policy. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff must not become "friends" with parents or pupils or former pupils on personal social networks such as Facebook, Twitter, Instagram or LinkedIn.

Use of Email – Staff are not permitted to use school email addresses for personal correspondence unrelated to school business. All email should be kept professional: whilst there can be no objection to a degree of informality in internal emails, the body text of any intended to go outside the school, for example to parents, should be composed no less rigorously than an old-fashioned letter. Staff are reminded that school data, including emails, is open to subject access requests under the DPA 2018.

Passwords - Staff should keep passwords private and never save these on school devices. There is no occasion when a password needs to be shared with another member of staff, pupil or IT support.

Data Protection – If it is necessary for staff to take work home, or offsite, they should ensure that any devices they intend to use are encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - Staff are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head, who will set the boundaries of personal use.

Images and Videos - Staff must not without consent upload on to any internet site or service images or videos of themselves, other staff or pupils. This is applicable not only professionally (in school) but also personally (e.g. staff social events).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head. (See Appendix V for guidance on use of personal devices).

Viruses and other malware - any virus outbreaks must be reported to the E-safety officer who will advise the Head and the Technical Support team as soon as is practicable to do so, along with the name of the virus (if known) and actions taken by the school.

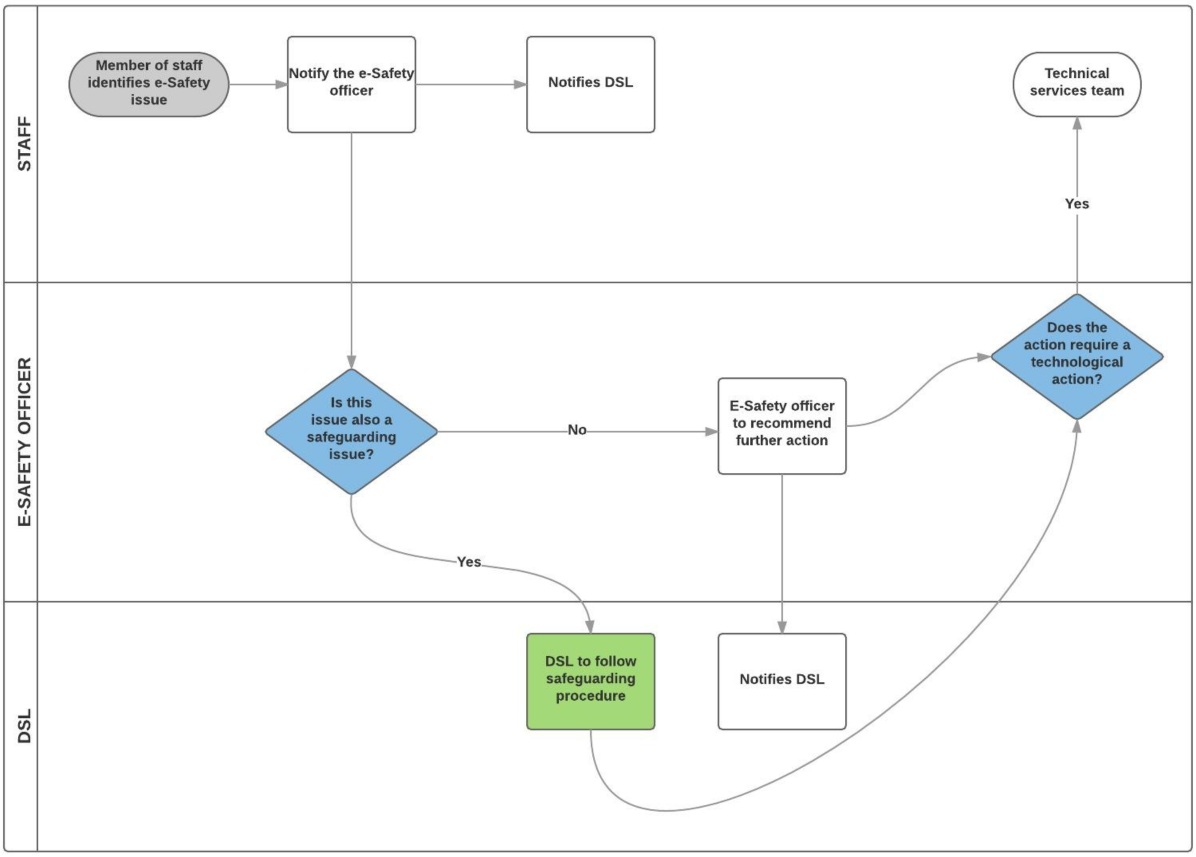
Social Media - E-safety – like health and safety, E-safety is the responsibility of everyone. As such staff will promote positive E-safety messages in all use of ICT whether they are with other members of staff or with pupils.

Any member of staff who suspects that a member of the school community is accessing inappropriate material or not abiding by the school's E-safety policy and protocols must report any allegation, complaint, concern or suspicion directly to the head. If the Head is absent or if the Head is the subject of the concern, the concern must be reported to the governor of the school.

APPENDIX III – INCIDENT PROCEDURES AND FLOWCHART

E-SAFETY FLOWCHART

Kevin Chung | June 3, 2016


STAFF
E-SAFETY OFFICER
DSL
Member of staff identifies e-Safety issue
Notify the e-Safety officer
Notifies DSL
Technical services team
Yes
Is this issue also a safeguarding issue?
No
E-Safety officer to recommend further action
Does the action require a technological action?
Yes
DSL to follow safeguarding procedure
Notifies DSL

APPENDIX VI - INFORMATION AND SUPPORT

There is a wealth of information available to support the school to keep children safe online. The following is not exhaustive but provides a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

APPENDIX VII - LEGISLATION AND GUIDANCE

The following guidance has been reflected in this policy.

- DfE statutory guidance in Keeping Children Safe in Education, September 2021
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- UK Council for Child Internet Safety (UKCCIS)
- The Data Protection Act 2018