Policy Name: Digital Safety
Policy Number: 12.1
Date: 1 September 2024

Table of Contents

1. Introduction

1.1 Sidcot School ("the School") is an independent mainstream boarding and day school for girls and boys aged from 3 to 18 years with a Quaker ethos. The School has an inclusive and celebratory approach to diversity and a strong pastoral system. The safety and wellbeing of all those in the School community, especially our children, is our primary concern.

1.2 This policy, and associated digital policies 12.2 (Digital Security) and Acceptable Use policies 12.3, 12,4 and 12.5 have been developed with this principle in mind, and are to be read in conjunction with the School's Child Protection and Safeguarding Policy (2.1), Staff / Student Code (2.2) and Anti-Bullying Policy (5.4).

1.3 Whilst the use of technology is now a key aspect of students' learning, it also carries with it significant safeguarding issues, including the risk of child sexual exploitation, radicalisation and sexual predation. Online bullying, sexting and other associated forms of harassment are also key concerns. This policy sets out the School's approach to safeguarding its students, and all those within the School Community, in respect of such matters, and also explains how the School complies with its duty to prevent people from being drawn into terrorism (known as the "Prevent Duty").

2. Scope and Distribution

2.1 This is a whole school policy including the EYFS. It applies to all members of the School Community, and to all those who have access, whether permanent or temporary, to technology at the School.

2.2 This policy is available on the School website, on the staff intranet and a hard copy can be provided free of charge from Sidcot School. It may also be made available in other formats upon request.

2.3 In this policy, the terms "child" "children" "pupil" and "student" are used interchangeably.

2.4 Please refer to paragraph 8 of the addendum to the Child protection and safeguarding policy which applies to school closure and arrangements for online supported learning which apply during pandemic situations. This paragraph details the measures that are required of staff to ensure the safety of students.

3. Responsibilities

3.1 The Governing Body of Sidcot School, in conjunction with the Senior Management Team (SMT), are responsible for ensuring the safety of all those in the School Community, especially students, and for responses to digital safety incidents that occur both in and outside of school and on school business, whether on personal or school networks or devices.

3.2 The Senior Management Team has developed this Policy, together with others in the digital space, and has oversight of issues regarding digital safety and digital security, and it monitors implementation of this Policy, including the

impact of digital safety, security and strategic initiatives. SMT are also responsible for regular reporting to the Governing Body.

3.3 Safeguarding is **everyone's responsibility,** although teachers have particular responsibilities as outlined in this Policy (in particular in paragraphs 5.4, 8.2.5 and 9.1.1 below), as they are directly involved with the students.

4. Safeguarding Technology and the School Environment

4.1 Digital Technology forms a central part of education at Sidcot School. We use computers in class, and the incidence of social media and smart devices impacts on the daily lives of the entire School Community. However, electronic ways of working and communication afforded by the School and personal devices present considerable dangers and risks, not least in respect of the personal safety of students, general treatment of others and security of data. To address such matters, the School has the following systems and processes in place:

- Filters to ensure that inappropriate sites are not accessible via the internet. The filters may be adjusted, where justified for educational purposes, and systems are in place to prevent over blocking (excessive filtering) to ensure that this does not lead to unreasonable restrictions as to what children can be taught online. The level of filtering is determined by a risk assessment addressing safeguarding issues, including the Prevent Duty;
- A change to the filtering level may be requested by any member of the School Community. This change request goes to the Head of IT Services, who will research the request and then make a recommendation to the DSL who will decide if the change should be made. Users are not permitted to use any program or software that might allow them to bypass the filtering/security systems in place and all users have a responsibility to report immediately to the DSL and/or the Head of IT Services any infringements of the filtering policy, or access to improper sites, of which they become aware;
- Monitoring systems proportionately which oversee internet use and inappropriate communication, and which flag up potential concerns whilst on site. No filtering system can guarantee complete protection against access to unsuitable sites, and the School therefore monitors activities of users and usage of its internet without prior notification to, or authorisation from, users. Users of the School's e mail and internet services cannot expect privacy in connection with anything they create, store, send or receive using the School's systems;
- Digital Safety and security education for students and training for staff (please see section 9 below);
- Oversight of use of technology during lessons;
- Reporting systems where there are incidents or concerns involving inappropriate use of technology, in particular where there are safeguarding concerns;
- A clear policy for the use of a wide variety of School-supplied and personal devices/equipment (please see section 7 below);
- The proper use of strong passwords, protection of data and regular reviews and audits of the safety and security of the School's technical systems;
- Appropriate security measures to protect servers, firewalls, routers, wireless systems, workstations, and mobile devices from accidental or malicious attempts which might threaten the security of the School systems and data.

These are tested regularly. The School's infrastructure and individual workstations are protected by up to date virus software;

- Managed Detection and Response (MDR) – 24/7 live monitoring of our systems is conducted by Sophos and allows real-time prevention of malicious actors

4.2. An outsourced IT partner is responsible for working with the School to ensure that the School's technical infrastructure is secure and is not open to misuse or malicious attack. The IT partner is responsible for ensuring that:

- The School meets the required Digital Safety technical requirements;
- Users may only access networks and devices through a properly enforced password protection policy, which requires that passwords be changed regularly;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- It is all users' responsibility to alert the Head of IT Services if any inappropriate sites can be (or have been) accessed;
- The School is kept up to date with digital safety technical information in order to effectively carry out the digital safety role and to inform and update others as relevant;

The use of the School network / Internet / Virtual Learning Environment (VLE) / Virtual Private Network (VPN) access/ email is regularly monitored and that monitoring software / systems are implemented and updated as required.

4.3 Specific rules are detailed in the following sections of this policy and the Digital Security Policy 12.2. However, for the avoidance of doubt, any safeguarding concerns arising from the use of technology in the school environment, or in connection with school activities, are to be reported/actioned in accordance with the School's Child Protection and Safeguarding Policy (2.1) and the Staff/Student Code (2.2).

4.4 The School's policy in relation to mobile phone use by staff in the Early Years Foundation Stage is set out in the Staff/Student Code Policy 2.2.

5. Anti-bullying (cyber-bullying), Sexting and Behaviour

Please refer to Anti – Bullying Policy 5.4 for the definition of bullying and further information.

5.1 The School is under a duty to look after the physical and mental health of its students and employees. This duty extends to safeguarding issues manifesting via the use of technology, in particular peer on peer abuse through cyber-bullying and/or sexting, and cyber-bullying of staff by students, parents and other members of staff. The School will support all involved in such incidents if they occur.

5.2 Cyber- (or 'virtual') bullying, sexting and other forms of digital harassment can occur in or outside school, at all times of the day or night, with a potentially bigger audience as people may forward content "at a click". The effects of such activity are well publicised in terms of the significant effects on mental health, partly as a result of the harmful communication effectively taking place within a child's home or venue outside school due to the reach of the internet. The School recognises that victims of harmful online behaviour can become marginalised or excluded by both on and offline communities, giving rise to the potential for repeat victimisation.

5.3 Sending or receiving a sexually explicit text or image or video of someone under 18 may amount to bullying and may constitute a criminal offence – even if it is taken with consent.

5.4 By law, the Head and staff, to such extent as is reasonable, are granted powers to regulate the behaviour of students when they are off the School site as well as on it, and to impose disciplinary penalties for inappropriate behaviour. Powers are also given to School staff with regard to the searching of electronic devices and the deletion of data in appropriate circumstances (please refer to section 10 below and to the School's Search and Confiscation Policy (5.10)). Such powers will be exercised in relation to incidents of cyber-bullying, or other digital safety incidents covered by this policy, the School's Behaviour Policies (5, 5.1a and 5.1b) and/or Anti-Bullying Policy (5.4), even where such incidents take place outside of the school, if they are linked to membership or activities of the School.

5.5 The School will, where appropriate and permissible, inform parents / carers of incidents of inappropriate Digital Safety behaviour that take place out of school.

5.6 In the event that cyber bullying or harassment is suspected of taking place, any person receiving the electronic information should take a screenshot or save the information and discuss with a class teacher, the DSL or relevant staff member who can decide on the next course of action and liaise with the DSL as appropriate.

6. General Use of Email and Internet Systems

6.1 Prohibited Email Use

6.1.1 It is prohibited for anyone to use the internet or e mail communication in any of the circumstances below:

a) Using software or web sites that attempt to hide internet activity for the purpose of evading monitoring;

b) Using the internet in any way that could bring the School into disrepute;

c) Distributing confidential information to unauthorised people or personal facilities;

d) Using third-party file sharing or transfer sites without prior authorisation, for example Dropbox;

e) Accessing web sites, publishing, downloading or transmitting content that can be reasonably interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or sites that deal with criminal activity, including (but not limited to) those involving or related to illegal drugs / substances, "legal highs", computer hacking/cracking, the creation of malicious software (malware), terrorism, and illegal weapons;

f) Using search terms that are likely to result in lists of, or images from, unacceptable web sites;

g) Harassing other people on the internet, or interfering in another member of the School Community's work. This includes, but is not limited to, the sending of unwanted e-mail, instant messages or chat messages;

h) Unauthorised use or distribution of copyrighted material, such as copyrighted music or movie content;

i) Downloading software without authorisation and an appropriate licence;

j) Using or acquiring computer utilities or tools that are primarily designed for gaining illegal access to other computer IT Systems (usually referred to as hacking or cracking tools);

k) Making unauthorised attempts to break into, or illegally access or damage, computer IT Systems or data;

l) Distributing (i.e. downloading or uploading) any form of malicious software;

m) Perpetrating or attempting to perpetrate any form of crime.

n) To contact students or staff on their personal email unless for legitimate reasons

a. Staff: For example when Furloughed

b. Students: once they have left the school and no longer have a school account

6.2 Viruses and Other Types of Malicious Software

6.2.1 Virus and other types of malicious software remain a serious threat to the School. All files, including .exe files, images, videos, spreadsheets and documents can carry viruses. It is still common for viruses to be spread via:

- Infected storage media (e.g. disks, memory sticks, etc.).
- Opening untrusted email attachments.
- Website links in malicious emails.

6.2.2 Viruses disrupt our daily business, waste time, can corrupt or destroy data, and may ultimately lead to financial loss and/or reputational damage.

6.2.3 Infected email messages often come from email addresses that the user does not recognise, but infected email messages from email addresses can also be received from known or recognised email addresses. People may be unaware that they have a virus infection when they send an email and many email borne viruses exploit people's contact lists to send out infected email messages automatically. In order to protect the School from viruses:

a) All storage media must be virus scanned before being used;

b) All members of the School Community should immediately report any sign or suspicion that a School computer is infected with a virus to the Head of IT Services;

c) No-one should forward any potentially malicious emails, even to the IT Department; this may only spread the infection. If in doubt, please verbally report the issue;

d) If in doubt, the IT department can check the safety of any files.

7. Mobile Devices

7.1 School Owned Devices

7.1.1 The School has provided technical solutions for the safe use of mobile technology for school devices.

- Appropriate access control is applied to all School supplied mobile devices according to the requirements of the user; this is done using a VPN;
- For all mobile technologies, filtering is applied to the Internet connection and attempts to bypass this are not permitted;
- All devices are subject to routine monitoring;
- The School will ensure that School devices contain the necessary apps for school work; they must remain on the School owned device in a usable condition and be easily accessible at all times. From time to time the School may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps;
- All apps added by the School will remain the property of the School.

7.2 Student Owned Devices

7.2.1 The School has implemented an age-appropriate scheme whereby students may undertake study using their own, School approved, mobile devices. Such devices remain the property of the student, and they, together with any other personal devices using the school system, are restricted through the implementation of technical solutions that provide appropriate levels of network access

7.2.2 Personal devices are brought into the School entirely at the risk of the owner;

7.2.3 The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or in use on activities organised or undertaken by the School (the School recommends insurance is purchased to cover that device whilst out of the home);

7.2.4 The School accepts no responsibility for the day to day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues;

7.2.5 The School recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the School. Pass-codes or PINs should be set on personal devices to aid security;

7.2.6 Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements;

7.2.7 Devices may not be used in public or mock examinations;

7.2.8 Photographs/images and videos may only be taken in accordance with section 8 of this policy,

7.2.9 Please refer to the Sidcot Blue Book for further guidance in terms of which Years and ages are permitted to bring their phones into school and where and when students are permitted to use them.

7.3 The Use of Cellular Data

7.3.1 Some personal electronic devices may allow internet access (e.g. 3G or 4G) or the creation of personal 'hotspots'.

7.3.2 Students must not connect to the internet or create a hotspot in this way by using their own device., They must not allow others to use their device or connect to their hotspot and will be responsible for the safety of their personal password.

7.3.3 Parents should be aware that if they provide their children with a 3G/4G/5G mobile device, they will be able to access the internet independently of the School system and therefore the School blocking and filtering system will not operate. The School values the support of parents in educating their children about digital technology and social media, alongside the work that the School undertakes

8. Use of Digital and Video Images

8.1 Use of Child Images for Identification and Security

All children are photographed on entering the school and, thereafter, annually, for the purposes of internal identification. These photographs identify the child by name, year group, house and form/tutor group. They are retained by the School in accordance with the principles detailed in the School's Digital Security Policy (12.2).

8.2 Safeguarding and Child Protection

8.2.1 No person is authorised to take images of children that:

- might cause embarrassment or distress
- are associated with distressing or sensitive issues
- are unnecessarily intrusive
- may expose an individual or the School to criminal or civil sanction

8.2.2 Subject to paragraph 8.1 above, images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected.

8.2.3 Photography is not permitted in sensitive areas such as changing rooms, toilets and swimming pools.

8.2.4 All children are encouraged to look after each other, and to report any concerns about the taking of images, misuse of technology, or any worrying issues. All reporting

should be made in accordance with the School's Child Protection and Safeguarding Policy (2.1).

8.2.5 Staff will be mindful of child protection issues and will raise concerns with the DSL (or any senior manager who is immediately available) if they become aware of anyone:

- taking an unusually large number of images
- taking images in inappropriate settings such as cloakrooms, toilets or changing areas
- taking images of children who are apparently unaware that they are being photographed or filmed.

8.2.6 Misuse of cameras or filming

Misuse of camera or filming equipment in a way that breaches this Policy, or the School's Anti-Bullying Policy, Digital Security Policy, IT Acceptable Use Policies, visitors and contractors' policy, or the school rules is always taken seriously, and may be the subject of disciplinary procedures or other action.

8.3 Consent

8.3.1 Upon admission to the School, written permission is requested from parents or carers (or, if the child is old enough, from the child him/herself) for the School to use or publish images/videos of children, both internally and externally, in certain limited circumstances, as detailed on the images consent form. In all other cases where the School wishes to use such images/videos, it will seek express written consent.

8.3.2 Where consent is required as above, the School will obtain such consent from the student provided they are of sufficient age and understanding to provide consent. Children aged 12 and above will normally be considered to be capable of giving or withholding consent themselves. In all other circumstances the parents' consent will be sought. In all cases, such consent will remain in force unless and until the School is informed otherwise.

8.3.3 A record of all consent details is kept securely on the MIS (SIMS). Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.

8.3.4 All images will remain on site at all times, unless prior explicit consent has been given by both the School Data Protection Lead and the parent or carer of any child or young person captured in any photograph. Should permission be given to take images off site, all relevant details are to be recorded, for example who, what, when and why and data will be kept securely. See also paragraph 8.5.2 below.

8.4 Use of Photographs by the School

8.4.1 Photographs and images are used to keep the School Community updated on the activities of the School, and for marketing and promotional purposes, including:

- on internal displays (including clips of moving images)
- on digital and conventional notice boards within school premises;

- in communications with the school community (parents, children, staff, Governors and alumni) including:
    - by email,
    - on the School intranet,
    - by post;
    - on the School's website and, where appropriate, via the School's social media channels, e.g. Twitter and Facebook.
- in the School's prospectus, and in online, press and other external advertisements for the School.

8.4.2 At all times, the School exercises care and sensitivity in its choice of images or videos which it wishes to use and the School will take reasonable steps to try to ensure that images are not reused without permission.

8.4.3 The School will not include any personal names, addresses, emails, telephone numbers, fax numbers on any video clip, on the website, in a prospectus or in any other printed publications.

8.4.4 Careful consideration is given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

8.4.5 On occasion the School will employ the services of a professional photographer to record certain events, in which case they will be asked to sign an agreement confirming compliance with this policy, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), that photographs will be used only for a specific purpose, subject to parental or student consent depending on the age of the student, and the photographer will be supervised at all times in line with the School's policies in respect of visitors and contractors.

8.4.6 Where practicably possible, the School will always notify parents in advance when the media is expected to attend a School event or activity in which school children are participating. The School will make every effort to ensure that any child whose parent or carer has refused permission for images of that child to be made aware in these circumstances are not to be photographed or filmed by the media. Identities of all press representatives will be verified, and every effort made to ensure that they comply with specific guidelines for any event.

8.4.7 The School sometimes records plays and concerts professionally including live streaming (or engages a professional photographer or film company to do so), in which case copies of the DVDs and CDs may be made available to parents for purchase. Parents of children taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

8.4.8 The School may from time to time use Unmanned Aerial Systems (UAS) - eg. drones - to record large events, such as sports days. Appropriate signposting will alert all attenders that filming will take place in certain areas. Images captured using a UAS will be subject to the retention and image sections of this policy and the Digital Security policy 12.2.

8.5 Retention, Storage and Destruction of Images and Data

8.5.1 In accordance with Data Protection principles, images will not be kept for longer than is considered necessary, and in all cases will be retained and deleted pursuant to the principles detailed in the School's Digital Security Policy (12.2).

8.5.2 Any memory stick, CD or storage device, or digital camera, storing images of children to be taken offsite for further work will be suitably encrypted and will be logged in and out by the by the member of staff issuing the photos, and monitored to ensure it is returned within the expected time scale.

8.5.3 Any "apps", websites or third party companies used to share, host or access children's images will be risk assessed prior to use by the School Data Protection Lead or such person nominated by them. The School will ensure that images are held in accordance with Data Protection law and that suitable child protection requirements are in place.

8.6 The Taking and use of Photos/Videos by Parents

8.6.1 The School understands that parents and carers may want to take photographs of their children during school performances, class assemblies, and other school events (such as sports day).

8.6.2 This is permitted by the School provided that images are taken purely for personal use. Courtesy and good manners require that the following rules are respected:

(i). Special attention is paid to the instructions given in any programme and/or by the teaching staff before or during school events/performances;
(ii). Video recordings are not taken except with express permission from the event organiser and strictly on the understanding that they are for personal use only; and,
(iii). Parents/carers shall ensure that they do not post images of children other than their own on social media without first gaining permission from the other children's parents/carers.

8.6.3 If the School becomes aware that any of the above conditions have been breached, it will take any action that it considers to be appropriate given the relevant circumstances. Parents and visitors should use common sense when taking images. If it seems appropriate to ask for someone's consent before taking images, permission must be requested and gained beforehand.

8.6.4 Parents should contact the School Data Protection Lead or, in accordance with the Child Protection Policy (2.1), DSL in the case of child protection and safeguarding issues, to discuss any concerns regarding the use of images.

8.7 Use of Photos/Videos by Children

8.7.1 On certain occasions children may take images of, and/or include, other children in images taken with their own digital equipment where a member of staff has explicitly authorised this. Parents should ensure that these images are shared only in line with this policy.

8.7.2 Photos taken by children for official use will only be taken with parental consent if the student is less than 13 years of age, or with the consent of the student if older than 13, and will be processed in accordance with the GDPR.

8.7.3 Parents and / or students will be made aware that children will be taking photos/videos of other children for official use and will be informed how these images will be managed by the School.

8.7.4 Still and video cameras provided for use by children and the images themselves will not be removed from the School.

8.8 Use of Closed-Circuit Television (CCTV)

8.8.1 CCTV cameras are appropriately placed within the School. All areas which are covered by CCTV are well signposted, and notifications are displayed so that individuals are advised before entering such areas. Where appropriate a data protection impact assessment will be undertaken by the Data Protection Lead, to assess the impact on the rights and freedoms of those whose images are being captured.

8.8.2 Recordings will be retained in accordance with the retention principles detailed in the Digital Security Policy (12.2), but in general for a limited time period only, and for no longer than their intended purpose. All recordings will be erased before disposal.

8.8.3 Regular auditing of any stored images is undertaken by the School Data Protection Lead.

8.8.4 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation. Requests from third parties should be made in writing to the Headmaster or the Data Protection Lead. However, consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.

8.8.5 Access to the CCTV recordings, software and data is strictly limited to authorised personnel, these being the Headmaster, Data Protection Lead, Head of Boarding and Director of Operations.

8.9 Use of Webcams

8.9.1 All areas which are covered by webcams for security or safeguarding purposes will be well signposted, and notifications displayed so that individuals are advised before entering such vicinity.

8.9.2 Recordings will be retained in line with the principles detailed in the Digital Security Policy (12.2), but in general for a limited time period only and for no longer than their intended purpose. All recordings are to be erased before disposal.

9. Training

9.1 Students

9.1.1 Digital safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. A broad Digital Safety curriculum is provided in the following ways:

- A planned Digital Safety curriculum is provided as part of Computing / PSHE / other lessons and is regularly revisited - visiting speakers also contribute to the programme as appropriate.
- Key Digital Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information;
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.;
- Where students are allowed freely to search the internet, staff are vigilant in monitoring the content of the websites they visit;
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff temporarily remove those sites from the filtered list for the period of study. Any request to do so should be in writing, with clear reasons for the need to relax filters, to the Head of IT Services.

9.2 Parents / Carers / Guardians

9.2.1 Parents, carers and guardians play an essential role in the education of their children and in the monitoring / regulation of their children's on-line behaviours. It is easy to underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and parents may be unsure about how to respond.

9.2.2 The School therefore seeks to provide information and awareness to parents and carers through:

- Newsletters, and the Parent Portal
- Occasional seminars organised by the DSL and their team
- Reference to the relevant web sites / publications e.g.
    - www.swgfl.org.uk
    - www.saferinternet.org.uk
    - http://www.childnet.com/parents-and-carers

9.3 Staff / Volunteers/ Contractors

9.3.1 It is essential that all staff understand their responsibilities, as outlined in this policy. Training is offered as follows:

- Digital Safety training is made available to staff. This is regularly updated and reinforced. It is expected that staff will identify Digital Safety as a training need within the performance management process if required.
- All new staff receive Digital Safety training as part of their induction programme, ensuring that they fully understand the School Digital Safety policy and Acceptable Use Agreements.
- The Head of IT Services, DPL and the DSL receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Digital Safety Policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days.

9.3.2 Volunteers are informed of their responsibilities upon their induction and supplied with the School policies to confirm their understanding.

9.3.3 Contractors and other visitors are informed of their responsibilities in line with policies 3.5 and 12.5.

9.3.4 The Head of IT Services, DPL & DSL will provide advice / guidance / training to individuals as required.

10. Searching and Deleting of any Device in School

10.1 Searches may be undertaken with the consent of the student or in the event that there is a suspected breach of the school rules or there is a suspected breach.

10.2 Where students are reasonably suspected of being in breach of the requirements of this or other School behaviour policies in relation to digital safety and security, authorised staff have the right to search electronic devices (or for them) in order to establish whether there has been a breach of School rules or policies, or the commission of an illegal act. Searches may be unrestricted where made with a student's prior consent. Where a student does not consent to a search, it may be made only for anything which is 'prohibited' under Section 550AA of the Education Act 1996, or otherwise banned under School rules.

10.3 Any breach of this or the acceptable use policy will invoke consideration of disciplinary sanctions in the behaviour policies.

Please refer to the search and confiscation policy (5.10) for further guidance regarding the grounds under which searches may be undertaken.

10.3 Examining Electronic Devices

10.3.1 During the course of a search, an authorised member of staff who locates an electronic device may access and examine any data or files on the device if they think there is a good reason to do so ("reasonable grounds").

10.3.2 The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

10.4 If inappropriate material is found on the device, it is the responsibility of the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or, where the material is of such a concerning / illegal nature, notify the police and other relevant agencies (for example social care). No one should view or forward illegal images of a child, but should refer to the police.

10.5 Where they are not involved already, any incident involving the search of a device and/or deletion of inappropriate material must be reported immediately to the DSL the DPL or the Head of IT Services

10.6 Authorised Staff

- The Head
- Deputy Headteacher(s)
- The Designated Safeguarding Lead
- The Deputy Safeguarding Lead(s)
- The Head of IT Services
- Data Protection Lead

10.7 Deletion of Data

10.7.1 Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

10.7.2 A record will be kept of the reasons for the deletion of data / files by the DSL. Head of IT Services

11. Schedule for Development / Monitoring / Review

11.1 The Digital Safety Policy will be regularly reviewed by the Senior Management Team, and approved by the Board at least annually at the Annual Safeguarding Review. Amendments will be made in accordance with updated guidance, practice or incident.

11.2 Members of the Group will monitor the implementation and impact of the policy by reviewing when required

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal data, for network activity
- The School's filtering policy and requests for filtering changes
- The digital safety curricular provision, in particular relevance, breadth and progression

12. Complaints

The School is always seeking to implement best practice and to strive for the highest standards. We operate an “open door” policy to discuss any concerns and the Digital Sidcot Group welcome suggestions and feedback. However, in the event of a complaint, policy 2.6 will apply and is available on the School website, school intranet, and in hard copy form free of charge.

13. Related Policies and References

2.1 Safeguarding and Child Protection Policy

2.2 Staff / student code (the staff behaviour policy)

2.6 Complaints

2.9 Educational trips and visits

3.1 Admissions

3.5 Procedure for visitors

4.4 Mental Health and Wellbeing

5.1, 5.1a, 5.1b, Behaviour

5.10 Search and Confiscation

5.11 Permanent Exclusions

7.1 PSHE

9.8 Staff disciplinary procedure

12.2 Digital Security

12.3 Acceptable Use (Staff)., 12.4 Acceptable Use (Students)

12.5 Acceptable Use (Visitors)

13.1 Related Legislation and Guidance

Legislation

The Education and Inspections Act (2006)

The Independent Schools Standard Regulations (2010)

The Equality Act (2011)

The Education Act (2010)

The Children Act (1989)

Protection from Harassment Act (1997)

Malicious Communications Act (1988)

The Communications Act (2003)

Public Order Act (1986)

Malicious Communications Act (1988)

Sexual Offences Act (2003)

Protection of Children Act (1978)

General Data Protection Regulation (2018)

Handbook for the Inspection of Schools – a commentary (ISI) (September 2020)

Keeping Children Safe in Education (Dfe September 2023)

Teaching Online Safety in Schools June 2019

Preventing and tackling bullying - Advice for headteachers, staff and governing bodies (Dfe October 2014)

Cyberbullying: Advice for headteachers and school staff (Dfe 2014)

Supporting Children who are bullied (Dfe 2014)

Mental Health and Behaviour in schools (Dfe March 2016).

Behaviour and discipline in Schools (Dfe 2016)

Prevent Duty Guidance (2015)

Counselling in schools: a blueprint for the future (February 2016)

Working Together to Safeguard Children (2018)

Sexual Violence and Sexual Harrassment between Children in Schools and Colleges (Dfe May 2018).

Searching, screening and confiscation – Dfe 2018

13.3 Related Websites:

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring

www.kidscape.org.uk

www.childnet.com

www.gov.uk/government/publications/preventing-and-tackling-bullying

https://www.thinkuknow.co.uk/ (CEOPs)

Appendix 1.

14. Digital Sidcot Group Members

- Safeguarding Governor

- Deputy Head Pastoral, Designated Safeguarding Lead, Digital Safety Co-ordinator, Head of Boarding and Prevent Duty Co-ordinator – SLT Joanna Leite

  Deputy Head Academic – SLT (Christian Hughes)
- Head of IT Services – SMT (Allison Clark)
- Data Protection Lead – SMT (Allison Clark)
- ICT Coordinator – Teacher (Matt Jarman)

15. Record of Changes

Changes	Person	Date
Consolidation of the e-safety policies into this policy to include updated statutory guidance from Keeping Children Safe in Education 2016.	James Russell	14/12/2016
Policy approved by Board in Board subject to further discussions at subsequent digital safety meeting	James Russell	20/01/2016
Updated with minor compliance changes, social media section moved to an appendix of the staff / student code	James Russell	25/01/20016
Personnel list and references updated Review and adopted by Board of Governors at Annual Safeguarding Review	Natalie Fear	07.10.2017
Policy rewritten to make it more concise Adopted by Board of Governors at Annual Safeguarding Review	James Russell / Chris Hobbs	06.10.2018
Reviewed, minor changes, and adopted by Governors at Annual Safeguarding Review	Natalie Fear / James Russell	05.10.2019

Reviewed, and adopted at Annual Safeguarding Review Additional paragraph inserted at para 2.4 which cross references the addendum to the child protection and safeguarding policy and details the arrangements for online supported learning during pandemic and other situations. Additional clarification at para 6 re prohibition of use of internet 10.3 Any breach of this or the acceptable use policy (which students are required to sign before using the ICT equipment) will invoke consideration of disciplinary sanctions in the behaviour policies. Reviewed and adopted by Board at Annual Safeguarding Review	James Russell Joanna Leite	18.09.2020 10.10.2020
Reviewed and approved by Board Alterations to paragraphs 8.8.4 and 8.8.5 regarding CCTV	Allison Clark/Keith Perry	08.10.2022
Reviewed, minor amendments and format changes	Allison Clark	25.09.2023
Reviewed and approved by Board as part of Annual Safeguarding Review		10.10.2023
Reviewed, minor amendments	Allison Clark	07.06.2024