RED HOUSE SCHOOL

# E-SAFETY AND PUPIL ACCEPTABLE USE OF ICT POLICY

This policy relates to all sections and activities of the school and its pupils, e.g. the Senior School, the Junior School (including EYFS), Wrap Around Care, Offsite Activities and School run Holiday Activities or Clubs. The policy also applies to incidents involving our pupils out of school hours.

## 1 INTRODUCTION

**1.1** Information and Communications Technology (ICT) in the twenty-first century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

**1.2** Guidance on how these skills can be developed safely are contained in Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (September 2023). This should be viewed in conjunction with our Child Protection (Safeguarding) Policy and the Department for Education updated guidance 'Filtering and Monitoring Standards for Schools and Colleges' (March 2023).

**1.3** ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

**1.4** Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email
- Instant Messaging and chat rooms
- Social media, including (but not exclusive to) Facebook, TikTok, Twitter, Snapchat and Instagram
- Smart phones and other mobile devices with web functionality
- Gaming, especially online
- Learning platforms and Virtual Learning Environments (VLE)
- Blogs and Wikis
- Podcasting
- Video and music broadcasting and downloading

**1.5** Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years.

**1.6** At Red House School, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

**1.7** Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage and potentially damage the reputation of the School.

**1.8** Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

**1.9** Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, ChromeBooks, iPads, laptops, mobile devices, webcams, digital video equipment, etc.); and technologies

owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

## 2 ROLES AND RESPONSIBILITIES

**2.1** The School is committed to safeguarding the welfare of all pupils and recognises that an effective E-Safety strategy is paramount to this. The School's responsibilities include:

**2.1.1** Focusing on online safety in all areas of the curriculum and reinforcing key online safety messages as part of assemblies and tutorial/pastoral activities, teaching pupils:

- About the risks associated with using the internet and how to protect themselves from potential risks.
- To be critically aware of content they access online and guided to validate accuracy information.
- How to recognise suspicious, extremist or bullying behaviour.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.
- How to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

**2.1.2** Ensuring that the School's staff act as good role models in their use of technologies, the internet and mobile electronic devices.

**2.1.3** Providing sufficient online safety training to staff to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety.

**2.1.4** Logging and monitoring online safety incidents on CPOMS and regularly reviewing this policy to ensure that the School's e-safety practices and procedures are adequate.

**2.2** As e-safety is an important aspect of strategic leadership within the school, the Head and the Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

**2.3** The Designated Safeguarding Leads (DSL) are Claire Thompson and Samantha Lindsay-Symington. The E-Safety Coordinators are Lucy Waldock (Junior School) and Graeme Butterfield (Senior School). The school's Network Manager is Graeme Butterfield. The E-Safety Coordinators report to the DSL. All members of the school community have been made aware of who holds these posts.

**2.4** The DSLs are responsible for understanding the filtering and monitoring systems Red House School has in place.

**2.5** In the Safeguarding and Child Protection training to all staff in September 2023, including the induction for new staff, the DSLs outlined to staff the expectations, applicable roles and responsibilities in relation to filtering and monitoring, as per KCSiE (September 2023).

**2.6** It is the role of the E-Safety Coordinators to keep abreast of current issues and guidance through organisations, such as, SLSCB (Stockton Local Safeguarding Children Board), CEOP (Child Exploitation and Online Protection) and Childnet.

**2.7** The Senior Management Team (SMT) and the Board of Governors are updated by the Head/E-Safety Coordinators and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

**2.8** This policy, supported by the School's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

**2.9** E-safety is linked to the following School policies:

- Child Protection (Safeguarding)
- Health and Safety
- Health and Safety – School Trips
- Behaviour Management
- Anti-Bullying
- Relationships and Sex Education (RSE)
- PSHE

**2.10** When using any form of ICT, including the internet, in school and outside school, it is the responsibility of all staff members to:

- Ensure all electronic communication with pupils, parents, staff and others is compatible with their professional role and in line with School policies.
- Not to talk about their professional role in any capacity when using social media, such as, Facebook and YouTube.
- Not to put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with their professional role.
- Use school ICT systems and resources for all school business, e.g. their school email address.
- Not to give out their own personal details, such as, mobile phone number, personal email address or social network details to pupils, parents, and others.
- Not to disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/or staff for professional purposes, in accordance with School policy and with the knowledge of the SMT.
- Not to browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that their online activity, both in school and outside school, will not bring Red House School or their professional role into disrepute.

## 3 MONITORING

**3.1** The Network Manager may inspect any ICT equipment owned or leased by the school at any time without prior notice.

**3.2** The Network Manager may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving Red House staff or contractors, without consent, to the extent permitted by law. This may be:

- To confirm or obtain school business related information.
- To confirm or investigate compliance with school policies, standards and procedures.
- To ensure the effective operation of school ICT.
- For quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998
- To prevent or detect crime.

**3.3** The Network Manager may, without prior notice, access the email account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

**3.4** All monitoring, surveillance or investigative activities are conducted by the Network Manager and comply with the Data Protection Act (1998), the Human Rights Act (1998), the Regulation of Investigatory Powers Act (2000) and the Lawful Business Practice Regulations (2000).

**3.5** Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

## 4 USE OF THE SCHOOL NETWORK AND INTERNET

### 4.1 Managing the Internet

**4.1.1** The School provides pupils with supervised access to Internet resources, through the School's fixed and mobile internet connectivity.

**4.1.2** Staff will preview any recommended sites before use.

**4.1.3** Raw image searches are discouraged when working with pupils.

**4.1.4** If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents check these sites the children are using and supervise this work. Parents will be advised to supervise any further research.

**4.1.5** All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

**4.1.6** All users must observe copyright of materials from electronic resources.

### 4.2 Infrastructure

**4.2.1** The School's internet access is controlled and monitored through the School's web filtering service. For further information relating to filtering please consult the Network Manager. The Network Manager (Graeme Butterfield) is responsible for ensuring appropriate filtering and monitoring systems are in place and he will regularly review their effectiveness. The Network Manager is aware of the need to block harmful and inappropriate content without unreasonably impacting teaching and learning. The Network Manager will meet with the DSL at least annually to review the School's filtering and monitoring provision.

**4.2.2** Red House School is aware of its responsibility when monitoring staff communication under current legislation and takes into account the following:

- Data Protection Act (1998).
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000).
- Regulation of Investigatory Powers Act (2000).
- Human Rights Act (1998).

**4.2.3** Staff and pupils are aware that school-based email and internet activity can be monitored and explored further, if required.

**4.2.4** The School does not allow pupils access to internet logs.

**4.2.5** The School uses management control tools for controlling and monitoring workstations.

**4.2.6** If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety Coordinator/Network Manager or teacher as appropriate.

**4.2.7** It is the responsibility of the School, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

**4.2.8** Pupils and staff are not permitted to download Apps, programs or files on school-based technologies, without seeking prior permission from the Network Manager.

**4.2.9** If there are any issues related to viruses or anti-virus software, the Network Manager should be informed.

**4.3** The following are not permitted:

- Damaging, degrading or disrupting computers, computer systems or computer networks or performance.
- Violating copyright laws.
- Using others' passwords.
- Trespassing in others' folders, work or files.
- Intentionally wasting resources.
- Any act which results in upheld complaints to, or legal action against, the School.
- Using the School network for illegal activity.
- Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Head and the SMT is unsuitable.
- Presenting documents compiled from Internet or School network resources as being the pupil's own work.
- Changing any of the computers' default settings, such as screensavers, backgrounds, folders, icons.
- Installing any software whatsoever.
- Circumvention of security or accounting provisions.
- The use of routers or dongles is banned in School, the access to WIFI rendering these devices unnecessary and a security risk to the School network.
- Malicious damage to or tampering with any system on the School network or changing of data.
- Transmission, creation or possession of threatening, extremist, defamatory or obscene material.
- Gaining unauthorised access to resources or websites by the use of internal/external wireless modems. Use of such devices to gain unfiltered access to the Internet is strictly forbidden.

## 5 ACCEPTABLE USE AGREEMENTS

### 5.1 Junior School pupils (EYFS and Key Stage 1 and 2)

- I will only use ICT in school for school purposes.
- I will only use my own school email address when emailing in school.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my E-Safety.

## 5.2 Senior School pupils (Key Stage 3 and 4)

### 5.2.1 Security and Privacy

- I will not disclose my password to others, or use passwords intended for the use of others.
- I will not use the computers in a way that harasses, harms, offends or insults others.
- I will not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- I will not download programs from the Internet nor have executable files in my network storage area.

### 5.2.2 Internet

- I will not access the Internet unless for study or for school authorised/supervised activities.
- I will not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- I will respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- I will not engage in 'chat' activities over the Internet.
- I will use my school Office 365 account for study or for school authorised activities only.

### 5.2.3 Electronic Devices

- I will use school iPads, Chromebooks, laptops or other electronic devices brought from home, such as smartphones, for educational purposes only.
- This includes the taking of pictures, and communications using these devices.

**5.2.4** A breach of the above will act as a failure to comply with the School's E-Safety and Pupil Acceptable Use of ICT Policy relating to the use of ICT facilities and electronic devices in school, and disciplinary action will be taken.

## 5.3 Staff, Governors and Visitors

**5.3.1** ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school.

**5.3.2** This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

**5.3.3** Any concerns or clarification should be discussed with Mrs Lucy Waldock (Junior School) or Mr Graeme Butterfield (Senior School), the School's E-Safety Coordinators, or the Head.

**5.3.4** I agree to the following:

- I will use the school's email/internet/intranet/learning platform and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will not accept as friends current pupils on a personal social network site.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware of software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or Head.
- I will not use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless using school owned storage devices, e.g. SD cards, or with the permission of the Head.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety and Pupil Acceptable Use of ICT and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

### 5.4 The implementation of the Acceptable Use Agreement

**5.4.1** Class teachers (Junior School) and Form Tutors (Senior School) will discuss the Acceptable Use Agreement with pupils at the start of each academic year.

**5.4.2** As part of the induction process, all new staff, governors and visitors who have been provided with access to the School's network, will be issued with the Acceptable Use Agreement, which they will be expected to sign. A copy of this will be kept within staff files by the Head of Finance and Compliance.

**5.4.3** A copy of the E-Safety and Pupils Acceptable Use of ICT Policy is on the School website.

## 6 MOBILE PHONES

### 6.1 Protocol in School

**6.1.1** Pupils from Year 6 upwards to Year 11 are allowed to bring a mobile to school. This includes:

- Pupils travelling to school by themselves.
- Pupils travelling by car by their parents.
- Pupils travelling to school via Red House organised transport.

**6.1.2** Pupils in the Junior School (Nursery-Year 5) are not permitted to bring a mobile phone into School.

**6.1.3** Pupils from Year 6 to Year 10 must hand their mobile phone in to their Form Tutor at 8.30am, at the start of morning registration, and must collect them from the Dining Hall at the end of the school day, unless they are given express permission by a staff member to use them in a lesson. Their mobile phone must be switched off and will be stored in a 'form' box in the Medical Room during the day. The Medical Room is kept locked.

**6.1.4** Pupils in Year 11 may keep their mobile phone about their person but they must be turned off during lesson times and at break time. The exception is that Year 11 pupils may use their phones at lunch time between 1.00-1.30pm when in the Year 11 Common Room (designated classrooms).

**6.1.5** Pupils in Years 6-11 who are attending Before School Care, Tea and Prep or a co-curricular club after school, may have their mobile phone in their pocket. However, the phone must be switched off.

**6.1.6** Parents of all Red House pupils, wishing to contact their children in an emergency, should always telephone the School Office and a message will be relayed promptly.

**6.1.7** If a pupil feels unwell during the school day, they must ask permission from their class teacher to go to the School Office to report their illness to Miss Ward. Miss Ward will then contact the parents directly. Pupils are not permitted to use their mobile phones to call their parents.

**6.1.8** In emergencies, pupils may request to use the school telephone. For example, if they've forgotten an essential piece of school equipment or medication.

**6.1.9** Parents must use the School Office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

**6.1.10** Pupils may not bring mobile phones, Smart Watches or any other wearables into examination rooms under any circumstances. If brought to the exam room by the pupil, they must be handed in before and then collected after the examination at the door.

**6.1.11** Pupils permitted to bring mobile phones onto School premises may only use it during School hours with express permission from their subject teacher, their form tutor, their Head of Years, or a member of the Senior Management Team (SMT) and they may be supervised.

**6.1.12** Pupils must not use mobile phones in any manner which in the reasonable opinion of the Head is inappropriate. Certain types of conduct, bullying or harassment can be classified as criminal conduct.

### 6.2 Mobile Phone use on fixtures, school visits and residential trips

**6.2.1** Pupils in the Junior School (Nursery-Year 5) are not permitted to take a mobile phone on a sports fixture, school visit or a residential trip.

**6.2.2** For pupils in Years 6-10, mobile phone use by pupils on sports fixtures, educational visits and residential trips is at the discretion of the member of staff leading the activity, and the expectations of the School must be explained to the pupils ahead of the activity taking place.

**6.2.3** Pupils in Year 11 are permitted to take a mobile phone on a sports fixture, school visit or a residential trip. The member of staff leading the activity, and the expectations of the School must be explained to the

pupils ahead of the activity taking place.

### 6.3 Sanctions for inappropriate mobile phone use

**6.3.1** The School takes such conduct extremely seriously, and will involve the police or other agencies as appropriate. Such conduct includes, but is not limited to:

- Sending/sharing of nude images.
- Upskirting.
- Threats of violence or assault.
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation.

**6.3.2** The School reserves the right to confiscate a pupil's mobile phone for a specified period of time if the pupil is found to be in breach of this policy. Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act (2006). If they are confiscated, the pupils will receive a sanction (demerit) in line with our Behaviour Management Policy.

**6.3.3** School staff have the power to search pupils' phones, as set out in the Department of Education's (DfE) guidance on Searching, Screening and Confiscation at School (updated 2022). The DfE guidance allows schools to search a pupil's phone if we have reason to believe the phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury.

**6.3.4** The pupil may also be prevented from bringing a mobile phone into the School temporarily or permanently and at the sole discretion of the Head.

### 6.4 Mobile phone loss, theft or damage

**6.4.1** Pupils bringing phones in to school must ensure that phones are appropriately labelled/identifiable.

**6.4.2** Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions.

**6.4.3** The School accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

**6.4.4** Confiscated phones will be stored in the Deputy Head's (Head of the Senior School) office in a secure location until collected by the pupil at the end of the school day.

**6.4.5** Lost phones should be returned to the School Office. The school will then attempt to contact the owner.

## 7 EMAIL

### 7.1 Managing email

**7.1.1** The School gives all staff their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

**7.1.2** It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. The school email account should be the account that is used for all school business.

**7.1.3** Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

**7.1.4** All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

**7.1.5** Pupils may only use school approved accounts on the school system and only under teacher supervision for educational purposes.

**7.1.6** Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act (2000). You must therefore actively manage your email account by organising email into folders and carry out frequent house-keeping on all folders and archives.

**7.1.7** Pupils have their own individual school issued email accounts from Years 2-11. This is the core mode of electronic communication between staff and pupils. Pupils in the Senior School from Year 5 upwards have a Microsoft Teams account. Pupils are encouraged to use this account and to check it on a daily basis.

**7.1.8** Pupils should not communicate with staff using private email accounts.

**7.1.9** Staff must inform the Network Manager if they receive an offensive email.

**7.1.10** Pupils are introduced to email as part of the ICT/Computing/Computer Science Scheme of Work.

**7.1.11** Staff must check their emails regularly, i.e. daily during term time, and if appropriate to their role, activate your 'out-of-office' notification when away for extended periods.

**7.1.12** Never open attachments from an untrusted source; consult the Network Manager first.

**7.1.13** For further information on staff email use, please read the Staff Email Policy.

## 8 CAMERA, PHOTOGRAPH AND VIDEO PROTOCOL

### 8.1 Taking of Images and Film

**8.1.1** Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

**8.1.2** Pupils in Years 6-10 are not allowed to operate mobile phones during school hours. They may only use cameras or other devices with the capability for recording and/or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

**8.1.3** Pupils in Year 11 may take images with cameras or mobile electronic devices with a camera facility only with the express permission of all those appearing in the image. This may only take place in the Year 11 Common Room (designated classrooms) at lunchtime between 1.00-1.30pm.

**8.1.4** All pupils must allow members of the School's SMT to access images stored on mobile phones and/or cameras and must delete images if requested to do so. This would only be done if the School had reason to believe that the image constitutes a breach of School discipline. This is in accordance with the DfE's guidance on Searching, Screening and Confiscation at School (2022).

**8.1.5** Posting of photographic material or videos, which in the reasonable opinion of the Head or a member of the School's SMT is considered to be offensive on websites such as YouTube, Instagram, Tik Tok, Facebook, Twitter etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the device used is a School computer, or a device operated elsewhere including the pupil's home.

**8.1.6** Cameras and mobile electronic devices with a camera facility may be confiscated and searched in appropriate circumstances, as per sections 91 and 94 of the Education and Inspections Act 2006 and the School's Behaviour Management Policy.

**8.1.7** If the Head or a member of the School's SMT has reasonable grounds to believe that a pupil's camera or mobile electronic device contains images, text messages or other material that may constitute evidence of criminal activity, they may hand the device to the Police for examination.

**8.1.8** Use of cameras or any mobile electronic devices with camera facilities in breach of this policy may result in confiscation of the equipment until the end of term and the pupil may be permanently banned from bringing a camera or mobile electronic device onto School premises in future.

### 8.2 Consent of Adults Who Work at the School

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

### 8.3 Publishing Pupil's Images and Work

**8.3.1** On a child's entry to the school, all parents, as part of the Parental Contract, are asked to give permission to use their child's photos or images.

**8.3.2** Pupils' first names are published against their image. Their full name is not published against their name, unless we have additional permission from parents. Email and postal addresses of pupils will not be published.

**8.3.3** Only the Head of Marketing, the Head of Admissions and the Marketing Assistant have authority to upload to the School website.

### 8.4 Storage of Images

**8.4.1** Images/films of children are stored on the School's network and secure cloud-based server.

**8.4.2** Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Head.

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

**8.4.4** Staff have the responsibility of deleting the images when they are no longer required.

## 8.5 Webcams and Closed-Circuit Television (CCTV)

**8.5.1** The School uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.

**8.5.2** We do not use publicly accessible webcams in school.

**8.5.3** Webcams in school are only ever used for specific learning purposes.

**8.5.4** Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

**8.5.5** Further information on the use of CCTV can be found in Appendix 3.

## 8.6 Video Conferencing and Remote Lessons

**8.6.1** The School uses Microsoft Teams for virtual meetings and lessons.

**8.6.2** This is covered by the Remote Teaching and Learning Guidelines.

# 9 PUPIL PERSONAL SAFETY

**9.1** Pupils must not:

- Use any type of social media to interact with people that they do not know in person.
- Reveal their home address, image, or phone numbers, or those of other pupils or of staff when online. They must use school addresses and phone numbers only.
- Arrange to meet someone that they have only met on the Internet or by email or in a chat room.
- Share their network password or allow others to use it.

**9.2** Pupils must:

- Use only their account and keep their password private.
- Create a strong password and change their password regularly.
- Report to an ICT Coordinator, teacher or Network Manager any unsolicited email, security problems, any unpleasant or inappropriate material, messages, or anything that makes them feel uncomfortable when online.
- Use social and blogging websites with great care being aware of the dangers that can be associated with posting pictures, text, opinions, videos and communications online.
- Make themselves aware of the security settings available when using social and blogging websites to protect personal information which is published online.

# 10 CYBERBULLYING

**10.1** Cyberbullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else.

**10.2** Any behaviour which seeks to intimidate or humiliate and which is repeated, intentional, malicious, such as to cause distress, unhappiness or insecurity, is strictly forbidden.

**10.3** Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

**10.4** Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Do not retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to evidence what is happening and can be used by the School to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving inappropriately.
- It is important to act. In the event that a pupil witnesses cyberbullying, it is important to support the victim and report the bully. If any pupil thinks that they, or another person, is being bullied, they should talk to a teacher or any trusted adult about the incident as soon as possible. For further guidance, see the School's Anti Bullying Policy.

**10.5** The website http://www.digizen.org/kids/ also provides useful support and resources to pupils who may feel uncomfortable with their use of the Internet. Other useful resources include:

- https://www.internetmatters.org/
- https://www.ceop.police.uk/safety-centre/
- https://www.issuesonline.co.uk/subscription/login
- http://www.saferinternet.org.uk/
- http://www.kidsmart.org.uk
- http://www.safetynetkids.org.uk/
- http://www.safekids.com/
- http://www.thinkuknow.co.uk

## 11 SAFEGUARDING AND PREVENT

**11.1** The School recognises that it has a duty under Section 26 of the Counter-Terrorism and Security Act (2015) to have due regard to the need to prevent people from being drawn into terrorism and to promote and safeguard the welfare of children and vulnerable adults (Education Act (2002), KCSIE (September 2023) and Prevent Duty Guidance: England and Wales (2023)).

**11.2** Staff are responsible for the wellbeing of the pupils and must ensure age appropriate material only is accessible via the school network by the use of filters.

**11.3** Any member of staff who feels someone is showing an interest in extremist, abusive or inappropriate material should report this to the DSL in the first instance. Any member of staff who believes pupils have access to inappropriate material should report this to the Network Manager.

## 12 SOCIAL MEDIA

### 12.1 School/staff use of social media

**12.1.1** The School uses Facebook and Twitter to communicate with parents. The Head of Marketing and Marketing Assistant are responsible for all postings on these technologies and on Facebook and other social media sites e.g. Twitter, Instagram and LinkedIn, monitors responses from others.

**12.1.2** Staff are not permitted to access their personal social media accounts using school equipment or their personal equipment during school hours.

**12.1.3** Staff are able to setup social media accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Facebook or other applications.

**12.1.4** Staff may, with the Head's permission, set up departmental social media accounts to promote the School.

**12.1.5** Staff may interact with School social media accounts i.e. liking on Facebook or retweeting on Twitter using their personal social media accounts. However, they should be aware that in doing so they will enable visitors to visit their own accounts and therefore privacy settings should be set to reflect this possibility.

**12.1.6** Staff may not mention the personal social media accounts of pupils or staff via any School social media account, as this exposes the account to the School's followers and may give visitors access to the account mentioned.

**12.1.7** Third party organisations that visit Red House School cannot take photographs of pupils and use them on their social media channels.

**12.1.8** The School may interact via social media with parents, prospective parents and past pupils. Interactions can include photographs; however, pupils must not be identifiable by their full name. The School can interact via social media with third party organisations, such as clubs which pupils attend outside of School. However, this is only if additional parental consent has been given. Interactions can include photographs; however, pupils must not be identifiable by their full name.

**12.1.9** Staff, governors, pupils, and parents are:

- Regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Aware that their online behaviour should at all times be compatible with the law.

**12.1.10** The School does not permit staff to accept as friends, current pupils on a personal social network site.

### 12.2 Pupil use of social media

**12.2.1** The use of social networking sites such as Facebook, Twitter, TikTok or similar sites is prohibited during the school day. The only exception is for Year 11 pupils between 1.00-1.30pm in the Year 11 Common Room (Room Q).

**12.2.2** Pupils must never make contact or chat to anyone who is not known to them and only invite known friends to chat rooms or alike.

**12.2.3** Pupils should only accept friendship requests from people they know in real life.

**12.2.4** 'Friend' requests must not be made to or by members of the School's staff.

**12.2.5** Pupils must consider how the images they share or comments they make may be used or viewed by others. Abusive or bullying language must never be used, nor should any other inappropriate language or comments be made.

**12.2.6** Pupils must not make comments about the School, staff members, other pupils or any other person that could be considered as defamatory or which could bring the School into disrepute. Behaviour of this kind will result in disciplinary action being taken in accordance with this policy and the School's Behaviour Management Policy.

**12.2.7** Inappropriate use of social networking sites may be reported to the site hosting it and inappropriate posts removed.

## 13 E-SAFETY IN THE CURRICULUM

**13.1** ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis.

**13.2** E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

**13.3** The School has a framework for teaching internet skills in ICT/Computing and Computer Science lessons.

**13.4** The School provides opportunities within a range of curriculum areas to teach about e-safety. For example, in assemblies and in PSHE/RSE lessons.

**13.5** Educating pupils about the online risks that they may encounter outside school is done when opportunities arise and as part of the E-Safety curriculum. For example, in assemblies and in PSHE/RSE lessons.

**13.6** Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

**13.7** Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.

**13.8** Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.

**13.9** Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or the CEOP report abuse button.

**13.10** Our staff receive regular information and training on E-Safety.

**13.11** New staff receive information on the School's Acceptable Use Agreement as part of their induction.

**13.12** All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

**13.13** All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

**13.14** We manage the School e-safety messages via the following methods:

- Embedding the e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- Class teachers and Form Tutors introduce the e-safety and Pupil Acceptable Use of ICT Policy to the pupils at the start of each school year.
- E-safety posters are prominently displayed around school, on both sites.
- Safer Internet Day is marked across the School on both sites every year.

## 14 GUIDANCE FOR PARENTS

**14.1** The School expects parents and guardians to:

- Promote online safety and to support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures.
- Talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour.
- Encourage their child to speak to someone if they are being bullied or need support.
- Encourage their child to adheres to this policy.

**14.2** Useful resources for parents include:

- www.internetmatters.org
- www.commonsensemedia.org
- www.thinkuknow.co.uk
- www.safeinternet.org.uk

**14.3** If parents have any concerns or require any information about online safety, they should contact the Head of the Junior School (for pupils in Nursery to Year 5) and the Deputy Head and Head of the Senior School (for pupils in Years 6-11).

## 15 PROCEDURES

**15.1** Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during lessons or at break or lunch time.

**15.2** Use of technology should be safe, responsible and legal. Violations of the rules in this policy will be dealt with in accordance with the School's Behaviour Management Policy.

**15.3** Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy.

**15.4** If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Child Protection (Safeguarding) Policy.

**15.5** If a pupil is worried about something that he/she has seen on the internet, he/she should talk to a teacher about it as soon as possible.

## 16 SANCTIONS

**16.1** Violations of the rules in this policy will result in a temporary or permanent ban from the School network.

**16.2** Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour in accordance with the School's Behaviour Management Policy, including confiscation of devices and, in the most serious cases, external suspension or expulsion.

**16.3** Any action taken will depend on the seriousness of the offence. When applicable, the Police or local authorities may be involved.

**16.4** The School reserves the right to charge a pupil or his/her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this policy.

## 17 MONITORING AND REVIEW

**17.1** All serious online safety incidents will be logged on CPOMS.

**17.2** The Network Manager and the Designated Safeguarding Lead have responsibility for the implementation and annual review of this policy and will consider the record of online safety incidents and new technologies, with the Safeguarding team where appropriate, to decide whether or not existing security and e-safety practices and procedures are adequate.

**17.3** The Head will report, annually, to the Board of Governors on the effectiveness of the School's E-Safety and Pupil Acceptable Use of ICT Policy.

Updated by: Miss C Thompson
September 2023

Ratified by: The Board of Governors
September 2023

## APPENDIX 1: CURRENT LEGISLATION

### 1 Acts Relating to Monitoring of Staff email

**Data Protection Act 1998**
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

**The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
http://www.hmso.gov.uk/si/si2000/20002699.htm

**Regulation of Investigatory Powers Act 2000**
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

**Human Rights Act 1998**
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

### 2 Other Acts Relating to E-Safety

**Racial and Religious Hatred Act 2006**
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

**Sexual Offences Act 2003**
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children and Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information www.teachernet.gov.uk

**Communications Act 2003 (Section 127)**
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**The Computer Misuse Act 1990 (sections 1-3)**
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files).
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program.
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

**Malicious Communications Act 1988 (Section 1)**
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

**Copyright, Design and Patents Act 1988**

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

**Public Order Act 1986 (sections 17-29)**
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

**Protection of Children Act 1978 (Section 1)**
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

**Obscene Publications Act 1959 and 1964**
Publishing an obscene article is a criminal offence. Publishing includes electronic transmission.

**Protection from Harassment Act 1997**
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## 3 Acts Relating to the Protection of Personal Data

**Data Protection Act 1998**
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

**The Freedom of Information Act 2000**
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

## APPENDIX 2: GUIDANCE ON PASSWORDS AND PASSWORD SECURITY

### 1 Passwords

- Always use your own personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to the Network Manager when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you are aware of a breach of security with your password or account inform the Network Manager immediately.

It is advised that:

- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 24 hours.

If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager.

### 2 Password Security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System (where appropriate) log-in username. They are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers or teachers. Online materials held in shared areas or on the i-drive are accessible.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Computers attached to the school's internet are automatically locked after 15 minutes of inactivity.

## APPENDIX 3: CCTV PROTOCOL IN SCHOOL

### 1 GENERAL

**1.1** This policy is in accordance with the requirements of the General Data Protection Regulation (GDPR) effective from 25 May 2018 and will be reviewed annually.

**1.2** The School's purposes of using the closed-circuit television (CCTV) system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

### 2 RESPONSIBILITY FOR CCTV SYSTEMS

**2.1** The Head has ultimate responsibility for the implementation and management of this Policy and will support the Head of Finance and Compliance in this respect.

**2.2** The Head of Finance and Compliance is responsible for the management of CCTV in respect of data protection matters.

**2.3** The School Secretaries and the Network Manager are responsible for the day to day management of the CCTV system.

### 3 POLICY STATEMENT

**3.1** Red House School uses CCTV images to provide a safe and secure environment for pupils, staff and visitors, and to protect school property.

**3.2** The purpose of this policy is to set out the position of the School as to the management, operation and use of the CCTV. This policy applies to all members of staff, visitors and all other persons whose images may be captured by the CCTV system.

**3.3** This policy takes account of all applicable legislation and guidance, including:

- The General Data Protection Regulation (GDPR).
- CCTV Code of Practice produced by the Information Commissioner.
- Human Rights Act 1998

### 4 PURPOSE OF CCTV

**4.1** The School uses CCTV for the following purposes:

- To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety.
- To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the site including deliveries and arrivals.
- To monitor staff and contractors when carrying out work duties.
- To monitor and uphold discipline among pupils in line with the Behaviour Management Policy.

### 5 SITING OF CAMERAS

**5.1** All CCTV cameras are fixed and sited in prominent positions where they are clearly visible to staff, pupils and visitors.

**5.2** Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The School will make all reasonable efforts to ensure that public areas are not recorded. Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as, the toilets.

**5.3** Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

### 6 MANAGEMENT AND ACCESS

**6.1** Access to stored CCTV images will only be given to authorised persons, under the supervision of the Head of Finance and Compliance.

**6.2** The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests.

**6.3** This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

**6.4** Individuals also have the right to access personal data the School holds on them in line with the School's Privacy Notice including information held on the system, if it has been kept (refer to Note 7).

**6.5** Authorisation to access CCTV images will be given:

- Where required to do so by the Head, the Police or some relevant statutory authority.
- To make a report regarding suspected criminal behavior.
- To enable the Designated Safeguarding Lead (DSL) or the Deputy Designated Safeguarding Leads (DDSL) to examine behaviour which may give rise to any reasonable safeguarding concern.
- To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents will be informed.
- To data subjects pursuant to a subject access request under Data Protection Law (GDPR).
- To the School's insurance company where required in order to pursue a claim for damage done to insured property.
- In any other circumstances required under law or regulation.

**6.6** Access to, and disclosure of, images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure that the images can be used as evidence if required.

**6.7** Images will only be disclosed in accordance with the purposes for which they were originally collected and a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

**6.8** Where images are provided to third parties above, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

## 7 SUBJECT ACCESS REQUESTS

**7.1** Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection legislation, and has a right to request access to those images. The request to access the data should be put in writing to the Head of Finance and Compliance.

**7.2** The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information).

**7.3** When such a request is made the Head of Finance and Compliance or their appropriately nominated representative will review the CCTV footage. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request.

**7.4** If the footage contains images of other individuals, then the School must consider whether the other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained. If not, is it otherwise reasonable in the circumstances to disclose those images to the individual making the request.

## 8 STORAGE AND RETENTION OF IMAGES

**8.1** Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

**8.2** For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event, will not be held for more than 31 days.

**8.3** Images stored on removable media such as CDs will be erased or destroyed once the purpose of the recording is no longer relevant.

**8.4** All digital recordings will be digitally watermarked to maintain integrity.

**8.5** A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Head of Finance and Compliance.

**8.6** An assessment will be made as to whether it is necessary to carry out constant real-time recording, or only at certain times when suspect activity usually occurs or is likely to occur.

**8.7** Cameras are maintained and serviced regularly to ensure they are kept in working order.

**8.8** In the event that cameras break down or are damaged, the Head of Finance and Compliance will be notified and will organise for the cameras to be repaired and working as soon as is practicable.

## 9 OTHER CCTV SYSTEMS

**9.1** The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or the Behaviour Management Policy.

## 10 TRAINING

**10.1** The Head of Finance and Compliance will ensure that staff handling CCTV images or recordings receive training on the operation and administration of the CCTV systems and, when doing so, comply with Data Protection Law.

## 11 MISUSE OF CCTV SYSTEMS

**11.1** The misuse of CCTV system could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

## 12 COMPLAINTS AND QUERIES

**12.1** Any comments or queries on this policy should be directed to the Head of Finance and Compliance using the School contact details.

**12.2** If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the School complaints/grievance procedure and should also notify the Head of Finance and Compliance.

**12.3** For any other queries concerning the use of your personal data by the School, please see the School's applicable Privacy Notice.

## APPENDIX 4 CCTV SMALL USER CHECKLIST

This CCTV equipment and the images recorded by it are controlled by the Head of Finance and Compliance who is responsible for how the system is used and for the notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement under Data Protection Law).

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes.

| | **Checked (Date):** | **Checked by:** | **Date of next review:** |
|---|---|---|---|
| The controller is aware that notification to the Information Commissioner is necessary and must be renewed annually. | | | |
| There is a named individual who is responsible for the operation of the system | | | |
| CCTV provides the best solution to the problems identified but this will be reviewed regularly. | | | |
| Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime. | | | |
| Cameras have been positioned to avoid capturing the images of persons not visiting the premises. | | | |
| There are signs showing that a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system. | | | |
| The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them. | | | |
| The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). | | | |
| Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties. | | | |
| The potential impact on individuals@ privacy has been identified and taken into account in the use of the CCTV system | | | |
| The operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment such as date and time stamp are correctly set). | | | |
| The controller knows how to respond to requests from individuals for access to images relating to that individual. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made. | | | |