E-Safety policy

Member of Staff Responsible	**CEO** (statement of intent for trust), **Headteacher** for procedure and implementation of e-safety at school.
Relevant guidance/advice/legal reference	KCSiE (2021)
Adopted by	Individual schools and trust office
Date of Policy	January 2022
Review Cycle	3 years
Date of Next Review	January 2025
Website	Yes (published annually)

Section 1 (Trust)

Statement of Intent (from the Trust)

This policy is not a statutory requirement, but its existence recognises the significance of students and staff remaining safe whilst accessing resources online.

The 3-18 Education Trust has the highest regard for E-safety in its schools in order to promote safe and responsible use of technology. We are committed to using new technology to enhance the curriculum and educational opportunities whilst equipping our children and young people with the knowledge and understanding to stay safe and vigilant when online, both in school and outside.

E-safety involves the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities through online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they should not access or it may lead to staff and students being treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside and is integral to a school's ICT curriculum. It may

also be embedded in Personal Social and Health Education (PSHE) and Relationships, Sex and Health Education and include how staff and students should report incidents

Advice and resources on internet safety are available at: https://www.saferinternet.org.uk/

In association with the relevant Acceptable Use Policy Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Child Protection and Behaviour policies

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable to regulate the behaviour of students when they are off the school site and (the Act) empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but which are linked to membership of the school.

Schools will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices.

The Prevent Duty (See Preventing Radicalisation and Extremism Policy)

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

https://www.educateagainsthate.com/

The use of devices in school, which are not owned by school

Mobile phones: If a student wishes to bring these into school, they must be switched off and put away (kept out of sight). The trust recognises the value that a mobile phone can have at the start and finish of the school day, but also the significant distraction and potential harm that the use of a mobile phone can bring when used in school.

Students found to be in breach of this requirement will have their device confiscated. These can be collected at the end of the day. If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated and the matter dealt with in line with normal school procedure (see below).

Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school has measures in place to prevent all forms of bullying. These measures should be part of the school's behaviour policy which are communicated to all pupils, school staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

Cyberbullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Section 2: School-based implementation and policy.

Individual schools are responsible for their E-Safety procedures and are given freedom to manage their provision. This is due to their different contexts with respect to key stages. Day to day responsibility for educating pupils in E-safety settings lies with the Headteachers and other staff with responsibility for the IT provision in schools.

The E-safety policy applies to all members of the school community, including staff, governors, pupils, volunteers, parents, carers, and visitors. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

Purpose

The purpose of this statement is to outline how the school will deliver safe and responsible use of ICT throughout school and give clear guidelines (Acceptable Use Agreements) to staff, pupils and volunteers.

1. **Responsibilities**

The member of the SLT team responsible for e-safety is: Katherine Mooney

The e-safety co-ordinator is: John Holmes

The e-Safety coordinator is responsible for working with the Pupil Related Matters Link, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the college community. He/she may also be required to deliver workshops for parents.

2. **E-Safety Committee is part of the Pupil Related Matters Link Committee**

It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils.

3. **Internet use and Acceptable Use Policies (AUP's)**

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. Examples of the AUPs used can be found in appendix 1.

A copy of the pupil AUP for primary and secondary phases will be available to parents via the website. This can be found in appendix 2

AUP's will be reviewed annually. All AUP's will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT in each Year group.

4. **Photographs and Video**

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, consent from parents must be gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering the use of images.

The Consent form used is in appendix 4.

Staff should always use a school camera to capture images and should not use their devices.

Photos taken by the school are subject to the Data Protection Act/GDPR.

The increased use of computing devices to assist with teaching particularly through lockdown periods has accelerated and necessitated, the operational policies to be put in place to ensure student parents and staff are kept safe. The use of video to deliver lessons is now more common. The trust is establishing a policy to support this.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their children at school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

5. **Mobile phones and other devices**

Pupils' mobile phones should be switched to silent whilst on the school premises. Pupil phones found to contravene this should be confiscated and sent straight to the school office. Confiscated phones can be collected by students, parents/carers after school.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal with the matter in line with normal school procedures.

6. **Use of e-mails**

Pupils should only use e-mail addresses that have been issued by the school and the email system should only be used for school-related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school-related matters.

7. **Security and passwords**

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

All users should be aware that the ICT system is filtered and monitored.

8. **Data storage**

Only encrypted USB pens are to be used in school. A safer way to store data is using the school systems which are now web-based.

9. **Reporting**

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents that may lead to child protection issues need to be passed on to the Designated teacher immediately – it is their responsibility to decide on appropriate action, not the class teachers.

Incidents that are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to SLT on the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Ceop button, trusted adult, Childline)

10. Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of the sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of the email
- Unauthorised use of the mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging/social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of the mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging/social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating the privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

11. Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. class commendation for good research skills, certificates for being good cyber citizens etc. Each year group coordinator will indicate these opportunities within the provided planning.

12. Social networking

Pupils are not permitted to use social networking sites within the school. See the separate School staff e-safety policy for guidance on staff use of social media.

13. Education

13.1 Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years. b). Regularly auditing, review and revision of the ICT curriculum
c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c). The school actively provides systematic opportunities for pupils/students to develop the skills of safe and discriminating online behaviour
d). Pupils are taught to acknowledge the copyright and intellectual property rights in all their work.

13.2 Staff

a). A planned programme of formal e-safety training is made available to all staff
b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
c). An audit of e-safety training needs is carried out regularly and is addressed
d). All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection/safeguarding procedures
e). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
f). Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
g). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
h). The school takes every opportunity to research and understand the good practice that is taking place in other schools
i). Governors are offered the opportunity to undertake training.

13.3 Parents and the wider community

There is a planned programme of e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety coordinator with input from the e-safety committee.

14. **Monitoring and reporting**

a). The impact of the e-safety policy and practice is monitored through the review/audit of e-safety incident logs, behaviour/bullying logs, surveys of staff, students /pupils, parents/carers

b). The records are reviewed/audited and reported to:

- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

c). The school action plan indicates any planned action based on the above.

Appendices

Appendix 1 – AUP’s

15. # AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher ○ never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

Signed _____

16. # AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit appropriate sites
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by the school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share legal content
- never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed _____

17. # AUP Guidance notes for learners in KS3 and above

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- set strong passwords which I will not share
- not use my mobile device in school unless I am given permission
- respect copyright and the intellectual property rights of others
- only create and share legal content
- always follow the terms and conditions when using a site
- only visit appropriate sites
- discuss and agree my use of a social networking site with a responsible adult before joining
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I am aware of the CEOP report button and know when to use it.

17.1 continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Trust/School policies, e.g. gambling
  - forward chain letters
  - breach copyright law
- do anything which exposes others to danger

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

18. # AUP for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public-facing site.
- only permit pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, eBay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer promote any supplied E-safety guidance

apropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling

- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off-site without permission from the headteacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

19. # AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e-Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately ○ parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit the use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

19.1 *St. Martin's School*

Parent/guardian name:……..
Pupil name: …….

(a) Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using filtered internet service, secure access to email, employing appropriate teaching practice and teaching esafety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting the safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's signature:…… **Date:**…….

Appendix 4 – Photo/video consent

Occasionally, we may take photographs of the children at our school. We may use these images in our school's prospectus or in other printed publications that we produce, as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use. From time to time, the media who will take photographs or film footage of a visiting dignitary or other high profile event may visit our school. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

To comply with the GDPR regulations, we need your permission before we can photograph or make any recordings of your child.

Please answer questions 1 to 4 below, then sign and date the form where shown.

PLEASE RETURN THIS COMPLETED FORM TO THE SCHOOL AS SOON AS POSSIBLE.

Please circle your answer

(1) May we use your child's photograph (unidentified) in the school prospectus and other printed publications that we produce for promotional purposes? Yes / No

(2) May we use your child's image (unidentified) on our website? Yes / No

(3) May we record your child's image (unidentified) on video or webcam? Yes / No

(4) Do you consent to your child being photographed or filmed in press events agreed by the school?
Yes / No

Do you consent to your child's full name being published with a press photograph? (At the present time, some local newspapers will not agree to publish a photograph without a full name). Yes / No

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies. Unidentified above means we will only use the first name.

Please also note that the conditions for use of these photographs are detailed overleaf.

I have read and understood the conditions of use overleaf.

Name of child: _____ Year Group:_____

Parent's or Carer's signature: _____ Date: _____

Parent's or Carer's Name (in block capitals):

_____

Conditions of school use

1. This form is valid for the period of time your child attends this school. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your agreement at any time. After the period of consent expires, the school will not use the images in further publicity material however the school may retain the images in an archive and would always endeavour to seek consent for any future use.
2. We, the school, will not use the personal details or full names (which means first name and surname) of any child in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.
3. We will not include personal e-mail or postal addresses, or telephone on video, on our website, in our school prospectus or in other printed publications.
4. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption, unless we have your agreement.

5. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.
6. We may include pictures of pupils and teachers that have been drawn by the pupils.
7. We may use group or class photographs or footage with very general labels, such as “a science lesson” or

“making Christmas decorations”.

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
9. As the child’s parents/guardian, we agree that if we take photographs or video recordings of our child/ren, which include other pupils, we will use these for personal and family use only. I/we understand that where consent has not been obtained from the other parents for any other use, we would be in breach of the GDPR if we used our recordings for any wider purpose including but not limited to social media

A full copy of the school’s privacy notice can be found on the school website, or please contact school and a hard copy can be provided.