Online Safety Policy

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

SAFEGUARDING AT MIDHURST CofE PRIMARY SCHOOL

Midhurst CofE Primary School is committed to Safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. Our intention is that children will be safe, secure and happy, and enjoy their time as pupils at this school.

During the writing of this policy due consideration has been given to all relevant aspects of Safeguarding and of children's welfare.

APPROVED (DATE)	NEXT REVIEW DATE
September 2024	September 2025

Mr Mark Jefferson - Headteacher

Mr Mark Purves - Chair of Governors

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Computing Lead/Headteacher and DSL's.

The Health & Safety Committee oversees online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL & deputies take joint lead responsibility for online safety in school, in particular:

- Supporting each other in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Computing lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Computing lead

The Computing lead (in conjunction with Agile) is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools

Primary schools insert:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via the school website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy/anti bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use other aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Year 5 and/or Year 6 pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headteacher/DSL's and Computing Lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures and staff handbook
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy

Acceptable Use and

Use of Digital / Video Images

Parental Permission for EYFS and KS1 Pupils

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

Digital technology is integral to the lives of children and young people, both within and outside school. These technologies are powerful tools, which can open new opportunities for everyone and promote effective learning. Young people should always have an entitlement to safe internet access.

Our Acceptable Use Policy is intended to ensure:

- that children and young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

At the beginning of each academic year (or at point of entry for mid-term joiners) class teachers will share, explain, and demonstrate our computing equipment and online safety rules to their class, before sending a copy home.

All pupils must follow the rules in this policy when using school computers, iPads, digital cameras, computing equipment, or the internet. Pupils who do not follow these rules will find:

- They are not allowed to use our computers or computing equipment,
- They can only use our computers or computing equipment if they are more closely watched.

This Is How I Will Use Computing Equipment in School Safely	
1	I will ask a teacher (or suitable adult) if I want to use the computing equipment.
2	I will only use activities that a teacher (or suitable adult) has told or allowed me to use.
3	I will take care of the computers, iPads and other computing equipment.
4	I will ask for help from a teacher (or suitable adult) if I am not sure what to do or if I think I have done something wrong.
5	I know that if I break the rules I might not be allowed to use the computing equipment.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified using their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Parents Photographing and Videoing Children at School

Parents may take photographs of school events subject to ordinary courtesies such as not obscuring the view of other audience members or distracting the children.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children

Acceptable Use for Home Learning During School Closure

Parents agree to use the Seesaw app to access home learning activities for their child in the event of school closure. The school will also email and text regularly during these times.

When learning is taking place at home, parents agree to ensure appropriate parental controls are in place on any devices used by their child. (Advice on how to manage this is available on the school website).

Children can communicate with teachers directly through the Seesaw app.

Parents agree that should their child need to contact the school or a member of staff during a period of school closure for extra advice or support, an adult either calls (01730 813526) or emails (office@midhurstprimary.co.uk) on their behalf.

Children may not contact members of staff directly via emails or by phone

Acceptable Use and

Digital/Video Image Parental Permission

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

I realize that any pupil under reasonable suspicion of not following these rules when using (or misusing) our computing equipment may have their use restricted, more closely monitored and/or past use investigated.

Parent / Carers Name _____ Pupil Name _____

- As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to computing systems at school.
- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed _____ Date _____

General Data Protection Regulation (GDPR) 2018: The above consents are in addition to the collection and sharing of data under GDPR 2018 as set out in our Privacy Notice. Any additional consent will be collected separately. If you wish to withdraw your consent at any time please contact the school office.

Acceptable Use and

Use of Digital / Video Images

Parental Permission for KS2 Pupils

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

Digital technology is integral to the lives of children and young people, both within and outside school. These technologies are powerful tools, which can open new opportunities for everyone and promote effective learning. Young people should always have an entitlement to safe internet access.

Our Acceptable Use Policy is intended to ensure:

that children and young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

At the beginning of each academic year (or at point of entry for mid-term joiners) class teachers will share, explain, and demonstrate our computing equipment and online safety rules to their class, before sending a copy home.

All pupils must follow the rules in this policy when using school computers, iPads, digital cameras, computing equipment, or the internet. Pupils who do not follow these rules will find:

- They are not allowed to use our computers or computing equipment.
- They can only use our computers or computing equipment if they are more closely watched.

This Is How I Will Use Computing Equipment in School Safely	
1	I understand that I must use school computing equipment and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the computing systems and other users.
2	I will use polite language and be responsible when using the computers. I will not use strong, aggressive, or inappropriate language and I will appreciate that others may have different opinions.
3	I must not write anything that might: deliberately upset someone or give the school a bad name.
4	I will not take or distribute photos/images of anyone without their permission.
5	I know that my teacher and the school will regularly check what I have done on the school computers.
6	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers in the past.
7	I must not talk to strangers online. I must not share any personal information - such as my name, where I live, my telephone number or my school - when I am online.
8	I must not tell my username and passwords to anyone else but my parents.
9	I must never use other people's usernames and passwords or computers left logged in by them.
10	If I think someone has learned my password then I will tell my teacher, or someone that works in the school.
11	I will log off after I have finished using any computer.
12	I know that online communication (e-mail, text and messaging) is not guaranteed to be private. I must not send unnamed e-mails.
13	I must not use the computers in any way that stops other people using them – by altering passwords and settings, downloading large files, printing large files etc..,
14	I will immediately report any unpleasant websites or online messages which make me feel uncomfortable, or which I think I should not be able to see, to my teacher, or an adult in the school. I will not show it to any other pupils.
15	I will tell my teacher or someone that works at the school immediately if I receive any messages that make me feel uncomfortable.
16	I will not try to harm any equipment or the work of another person on a computer.
17	I understand that the school computing equipment is to be used to help my learning and I will not use it for personal or recreational use, unless I have been given permission.
18	I know that if I bring a personal device (mobile phone, iPad, USB etc) into school I may not use it during the school day, unless I have been given permission to do so by a teacher and if I do use my own device, I will follow the rules set out in this agreement as if I was using school equipment.
19	I understand the risks and will not try to upload, download or access any information or images which are illegal or inappropriate or may cause harm or distress to others.
20	I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such information or images.
21	I will immediately report any damage or faults involving equipment or software, however this may have happened.

22	I will not install or attempt to install or store programmes of any type on any school device. I will not try to alter computer settings.
23	I will not access any social media sites whilst at school.
24	I should ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not try to download copies (including music and videos).
25	When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be accurate.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified using their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Parents Photographing and Videoing Children at School

Parents may take photographs of school events subject to ordinary courtesies such as not obscuring the view of other audience members or distracting the children.
Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

Acceptable Use for Home Learning in the event of School Closure

Parents agree to use the Seesaw app to access home learning activities for their child in the event of school closure. The school will also email and text regularly during these times.

When learning is taking place at home, parents agree to ensure appropriate parental controls are in place on any devices used by their child. (Advice on how to manage this is available on the school website).

Parents agree that should their child need to contact the school or a member of staff during a period of school closure for extra advice or support, an adult either calls (01730 813526) or emails (office@midhurstprimary.co.uk) on their behalf.

Children may not contact members of staff directly via emails or by phone.

Parents agree that if a member of staff arranges a phone call with a family/child during a period of school closure, that it will be to a landline or a parent's mobile and that a parent/responsible adult will be present for the duration of the call.

Acceptable Use and Digital/Video Image Parental Permission

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

Parent / Carers Name _____ Pupil Name _____

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to computing systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. Yes / No

Signed _____ Date _____

General Data Protection Regulation (GDPR) 2018:
The above consents are in addition to the collection and sharing of data under GDPR 2018 as set out in our Privacy Notice. Any additional consent will be collected separately.

If you wish to withdraw your consent at any time please contact the school office.

Staff, Governors and Community Users
Acceptable Use Policy and Agreement
(Including Use of Digital/Video Images)

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

School networked resources, including Bromcom and Bromcom Learning Gateway, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the computing co-ordinator.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos, code of conduct and behaviour, e-safety and safeguarding policies.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff, governors and community users under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact computer co-ordinator.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will not continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to computer co-ordinator.
15	I will not use "USB drives", portable hard-drives, tablets or personal laptops on the network without having them "approved" by the school and checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.
19	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held in Bromcom.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.

23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet (or taken offsite in any other way) will be encrypted or otherwise secured.

Additional guidelines:

Staff, governors and community users must comply with the acceptable use policy of any other networks that they access.

COMMUNICATIONS

In school, staff, governors and community users' communication on own or school mobile devices is subject to the following regulations:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	☑						☑	
Use of mobile phones in lessons				☑				☑
Use of mobile phones in social time		☑						☑
Taking photos on mobile phones or other camera devices				☑				☑
Use of hand held devices eg PDAs, PSPs				☑			☑	
Use of personal email addresses in school, or on school network	☑							☑
Use of school email for personal emails	☑							☑
Use of chat rooms / facilities				☑				☑
Use of instant messaging		☑						☑
Use of social networking sites		☑						☑
Use of blogs	☑						☑	

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data because of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the computer co-ordinator immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the computer co-ordinator. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

The office holds a complete list of those children who may not be photographed.

USE OF DIGITAL / VIDEO IMAGES POLICY

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

Aims

We aim to use photographs and cameras at Midhurst C of E Primary School for:

• Assessment, planning and recording

• Observation tools

• Information for visitors and parents

• Training purposes

• Language extension

• Teaching and learning resources (with links to Computing and Global Awareness)

USE OF PHOTOGRAPHS

Photographs are used extensively throughout Midhurst C of E Primary School for a variety of purposes. Generally, staff take photographs of the children throughout the year to capture a particular example of play or something that a child has achieved. In addition, we use photographs for:

Photographs	Purpose
Displays of children's work	A record of ideas and topic references for future use
Examples of children's play	As a part of an individual child's profile given to parents at the end of the year.
Classroom areas	To show the range of activities there for visitors and parents
Class albums	For children to look at and talk about
School policy folders	To explain the work of the school to parents and visitors
Special events and festivals	As a record of the school year and for children and parents to look at and talk about
Birthday display	Used as a class resource for talking about birthdays, months of the year etc
Photographic maps of the school and local environment	A resource for topic work usually focused in on Knowledge and Understanding of the World
From home in the All About Me booklets	To act as a link between home and school when the children start at Midhurst
Children's own photographs	Children take photographs at school often on the digital camera, to gain experience in using technology

Camcorders are also used in school for many of the above purposes. In particular we may use them for observations of children's play to further our understanding, or for assessment and planning tools.

POINTS TO CONSIDER

We are aware of the need for sensitivity when taking photographs and observe the following:

The child does not object to having his/her photograph taken.

Photographs are used to show positive issues (e.g., a piece of work that the child has worked hard on or is pleased with, children playing cooperatively together…….)

We are inclusive so that gender, race, Special Educational Needs, and differing abilities are reflected in a balanced way.

There may be cultural issues of which we need to be aware when taking photographs of children from different ethnic minority groups.

Where photographs, videos or even samples of children's work are to be displayed outside school we seek parental permission for this to happen. (See Permission and Copyright Release Letter) Examples of this are newspaper reports, articles in education publications or exhibitions of children's work.

Students, Governors, Community Users or visiting professionals or researchers who need to take photographs or videos as part of their work, are made aware of the need for confidentiality and that children will not be named or identified in any other way.

Parents are made aware of our use of cameras, and the location of this policy through the school prospectus and have the opportunity to voice any concerns.

Parents Photographing and Videoing Children at School

Staff, Governors and Community Users may take photographs of school events subject to ordinary courtesies such as not obscuring the view of other audience members or distracting the children.

Parents /carers are requested to sign a permission form to allow the school to take and use images of their children. It is the responsibility of Staff, Governors and Community Users to check with the school office if the children in question have permission for digital images to be used.

Acceptable Use for Home Learning During School Closure

Parents agree to use the Seesaw app to access home learning activities for their child in the event of school closure. The school will also email and text regularly during these times.

When learning is taking place at home, parents agree to ensure appropriate parental controls are in place on any devices used by their child. (Advice on how to manage this is available on the school website).

Children can communicate with teachers directly through the Seesaw app.

Parents agree that should their child need to contact the school or a member of staff during a period of school closure for extra advice or support, an adult either calls (01730 813526) or emails (office@midhurstprimary.co.uk) on their behalf.

Children may not contact members of staff directly via emails or by phone.

Parents agree that if a member of staff arranges a phone call with a family/child during a period of school closure, that it will be to a landline or a parent's mobile and that a parent/responsible adult will be present for the duration of the call.

Staff, Governors and Community Users Acceptable Use Agreement

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt, I will consult the computer co-ordinator.

I agree to report any misuse of the network to the computer co-ordinator.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the computer co-ordinator.

Lastly, I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the computer co-ordinator.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I agree that if I take digital or video images at, or of, school events which include images of children, I will abide by these guidelines when taking and in my use of these images.

Name of member of Staff, Governors or Community User

Signed

Date

General Data Protection Regulation (GDPR) 2018:

The above consents are in addition to the collection and sharing of data under GDPR 2018 as set out in our Privacy Notice. Any additional consent will be collected separately.

If you wish to withdraw your consent at any time please contact the school office.

Online Safety Policy

Midhurst C of E Primary School
LIFE IN ALL ITS FULLNESS

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**