



Markyate Village School and Nursery

Online Safety Policy 2024

<u>Staff Responsible for Review</u> Head Teacher, DSL/DDSL, Senior Leadership Team	
<u>Last Review</u> September 2024	<u>Date of Next Review</u> September 2025
<u>Approved by Governing Body</u> September 2024	<u>Review Cycle</u> Annually

Contents

1. Introduction.....	1
2. Responsibilities.....	1
3. Scope of Policy and Aims	3
4. Policy and Procedures.....	3
4.3 Storage and propagation of Images	5
4.4 Use of personal mobile devices (including phones)	6
4.5 Staff Using work devices outside of school	6
4.6 Reporting incidents, abuse and inappropriate material.....	7
4.7 Cyber-bullying	7
5. Curriculum	8
6. Staff and Governor Training	9
7. Working in Partnership with Parents/Carers	9
8. Records, Monitoring and Review	10
9. Appendices of the Online Safety Policy.....	11
A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff) 11	
B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers	11
Appendix A -Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)	12
Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers and other personnel working with children on the school grounds.	15
Appendix C - Requirements for visitors, volunteers and parent/carers helpers.....	18
Appendix D - Online Safety Acceptable Use Guide, Primary Pupils	19
Appendix E - Online safety policy guide - Summary of key parent/carers responsibilities	21
Appendix F - Guidance on the process for responding to cyberbullying incidents	22
Appendix G - Guidance for staff on preventing and responding to negative comments on social media.....	23

1. Introduction

Markyate Village School recognises that internet, mobile and digital technologies provide opportunities for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

2.1 The On-Line Safety Governor

The On-Line Safety Governor will monitor online safety logs as provided by the Designated Safeguarding Lead (DSL), Anna Page.

The Governor who oversees online safety is Victoria Horsnall

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 A)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Head Teacher

The Head Teacher 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 (DSL) and Deputy Designated Safeguarding Leads (DDSLs)

Details of the school's DSL [and deputies] are set out in our child protection and safeguarding policy as well as in job descriptions.

DSLs take responsibility for online safety in school, including:

- Working with Herts for Learning Data Manager Service (who act as the ICT Manager for the school) 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;
- Logging all incidents of cyber-bullying and managing them appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety (DSL);

- Liaising with other agencies and/or external services if necessary;
- Providing termly reports on online safety in school to the Head Teacher, Pastoral Committee and Full Governing Board;

3.4 The ICT Manager (Herts For Learning Data Management Service)

Responsibilities for HfL Data Management Service include:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems;
- Reviewing and updating their security procedures termly 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 ICT systems are secure and protected against viruses and malware, and update such safety mechanisms regularly; the School Business Manager and Headteacher will review these at fortnightly Premises Meetings
- Blocking access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files;

3.5 All staff and volunteers

The responsibilities of all staff, including contractors, agency staff and adults volunteering in school, includes:

- Understanding this policy and implementing this policy consistently;
- Agreeing to the terms on acceptable use of the school's ICT systems and the internet (Appendix A for Staff and B and C for contractors and volunteers);
- Ensuring that pupils follow the school's terms on acceptable use (Appendix D) on arrival to the school, with paperwork held in Class Folders;
- Working with the DSL to record all online safety incidents;
- Following the Child Protection Policy for reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here'.

3.6 Parents

The responsibilities of parents includes:

- Notifying a member of staff or the Head Teacher of any concerns or queries regarding this policy;
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix D).

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](#)
- Developing respectful relationships – [Disrespect Nobody](#)

3.7 Visitors and members of the community

The Head Teacher will make visitors and members of the community who use the school's ICT systems or internet aware of this policy, when relevant. The Head Teacher will ensure that visitors agree to the terms on acceptable use (Appendix C).

3. Scope of Policy and Aims

The policy applies to:

- Pupils;
- Parents/carers;
- Teaching and support staff;
- School governors;
- Peripatetic teachers/coaches, supply teachers, student teachers;
- Visitors;
- Volunteers;
- Voluntary, statutory or community organisations using the school's facilities.

The school provides online safety information for parents/carers through the website, in newsletters and at events, to help support parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, protects the interests and safety of the whole school community. It is linked to the following other school policies and documents: Safeguarding; GDPR; Health and safety; Home–school agreement; Behaviour; Anti-bullying; and PSHCE/RSE.

Our school promotes:

- Processes to ensure the online safety of pupils, staff, volunteers and governors;
- Approaches 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’);
- 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, anti-Semitism, 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 scam

4 Policy and Procedures

The school ensures that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

4.1 Use of email

- Staff and governors use a school email account or Governor Hub for all official communication to ensure everyone is protected through the traceability of communication;
- Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address;
- Pupils only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR;
- Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000;
- Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to the Head Teacher;

Users must not:

- Take part in cyberbullying by sending emails which are offensive, embarrassing or upsetting to anyone.

4.2 Visiting online sites and downloading

- Staff preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff consult with the Data Protection Officer (DPO) with details of the site/service. If internet research is set for homework, staff will give the names of sites that have been checked by the teacher. All users observe copyright of materials from electronic sources;
- Staff only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families;
- When working with pupils, staff search for images through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download , upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative);
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative);
- Adult material that breaches the Obscene Publications Act in the UK;
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status;
- Promoting hatred against any individual or group from the protected characteristics above;
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy;

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel, offensive language and disrespect;
- Reveal or publicise confidential or proprietary information;
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses;
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given by the on-line safety co-ordinator;
- Use the school's hardware and Wi-Fi facilities for running a private business;
- Intimidate, threaten or cause harm to others;
- Access or interfere in any way with other users' accounts;
- Use software or hardware that has been prohibited by the school.

Only a school device may be used to conduct school business outside of school unless explicit permission has been given by the Head Teacher. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Head Teacher.

4.3 Storage and propagation of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

The school stores photographs and images of pupils on the school's agreed secure networks which include some cloud based services. It restricts rights of access to stored images to approved staff as determined by Senior Leadership team. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

4.4 Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas. Mobile phones must not be used in a classroom in the presence of pupils.

Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers and FOMS (Friends of Markyate School) should not use their mobile phones on the school playgrounds or outside areas. They may only use personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Head Teacher.

When hosting an event where parents are permitted to take photographs or videos, it is made clear from the start by a member of staff that any images taken must be for private use only and if they include others, they must not be put on the web/internet without their consent; otherwise Data Protection legislation may be contravened.

The school office reminds parents/carers coming onto school premises but not in a designated area, that their phone/s must be out of sight.

Year 6 pupils are allowed to bring personal mobile devices/phones to school but they must not be switched on when on the school site. On arrival to school, such devices are switched off and handed in to a member of staff who will ensure the device is kept in a secure location during the school day. Under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil while on the school site.

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Any such content found must be reported to the Head Teacher or Deputy Designated Safeguarding Leads immediately.

Due to data protection risks, the school recommends that staff do not use personal mobiles to access school emails and data. If a member of staff does use their mobile phone to access school data or email, he / she must follow the security steps set out in section 4.5 of this policy and be aware of the data protection risks. If a member of staff does not follow the security guide-lines they will be in breach of the policy. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

4.5 Staff Using work devices outside of school

All staff members take the following steps to ensure their devices are secure by:

- 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 share the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Not saving the passwords in the browser;
- Use devices that are password protected;
- Keeping operating systems up to date – always install the latest updates;

Staff members must not use the device in any way that would violate the school's terms of acceptable use, ([Appendix A](#)) .

4.6 Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the Head Teacher or Leadership team. Where such an incident may lead to significant harm, staff follow the school's safeguarding procedures. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

4.7 Cyber-bullying

4.7.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

4.7.2 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. Class teachers discuss cyber-bullying with their tutor groups.

Teaching staff find opportunities to use 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).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the Head Teacher or Deputy Designated Safeguarding Leads 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 considers whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

4.7.3 Examining electronic devices

Staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm; and/or
- Disrupt teaching; and/or
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material; or
- Retain it as evidence (of a criminal offence or a breach of school discipline); and/or
- Report it to the police*.

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on [screening, searching and confiscation](#);
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#);
- The school's COVID-19 risk assessment;

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

5 Curriculum

In **Key Stage 1**, staff teach pupils 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** staff teach pupils 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 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.

Specific curriculum areas:

- Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism particularly in Key Stage 2;
- The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge;
- It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

6 Staff and Governor Training

- The Head Teacher ensures that staff are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records;
- The Head Teacher will provide new staff with a copy of the Online Safety Policy and sign the school's Online Safety Acceptable Use Agreement (Appendix A)
- Governors are responsible for completing on-line safety training as provided through Herts for Learning. Their training is recorded on Governor Hub and monitored by the Safeguarding Governor at the Full Governing Body (FGB) termly meetings.
- Peripatetic teachers/coaches and volunteers working with children on the school grounds are provided with a copy of the Online Safety Policy and are required to read and sign the Online Safety Acceptable Use Agreement (Appendix B and C); supply teachers are given the Safeguarding guidance information when arriving in school by the Business Manager

7 Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks regularly to consult and discuss online safety with parents/carers and to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Class Teachers ask parents/carers annually to read, discuss and co-sign with each child the Home School Agreement which explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8 Records, Monitoring and Review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported to the Head Teacher or Deputy Designated Safeguarding Leads via the On-Line Safety Incident Record and logged on CPOMS (for pupils or parents / carers) or staff file. For serious breaches, the Head Teacher may also log breaches with the Local Authority Designated Officer (LADO). All staff have the individual responsibility to ensure that incidents are correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9 Appendices of the Online Safety Policy

- A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
- B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches
- C. Requirements for visitors, volunteers and parent/carers helpers working in the school (working directly with children or otherwise)
- D. Online Safety Acceptable Use Guide, Primary Pupils
- E. Online safety policy guide - Summary of key parent/carer responsibilities
- F. Guidance on the process for responding to cyberbullying incidents
- G. Guidance for staff on preventing and responding to negative comments on social media

Appendix A

Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff role)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Head Teacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the School leadership team.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will take images, sound recordings or videos of school events or activities where specific permission has been granted.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Head Teacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices unless a closed, monitorable system has been set up by the school.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the school admin team.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or leadership team.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the school leadership team.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature Date

Full Name (please use block capitals)

Job title

Appendix B

Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches and other personnel working with children on the school grounds.

School name: Markyate Village School

Online safety lead: Victoria Hornsall

Designated Safeguarding Lead (DSL): Anna Page

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the school leadership team. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's On-Line Safety Policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the leadership team.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Head Teacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Head Teacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the Head Teacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand

that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the school admin team.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or Leadership team.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Head Teacher or Deputy Head Teacher.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature Date

Full Name (Please use block capitals)

Job Title/Role

Appendix C - Requirements for visitors, volunteers and parent/carers helpers (Working with technology in school)

School name: Markyate Village School

Online safety lead: Victoria Hornsall

Designated Safeguarding Lead (DSL): Anna Page

Deputy Designated Safeguarding Leads (DDSL): Libby Karmock, Sarah Partridge, Deborah Cobb

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSL or Head Teacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix D - Online Safety Acceptable Use Guide for Primary Pupils

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.

- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Appendix E - Online safety policy guide - Summary of key parent/carers responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Home School Agreement which includes online safety guidance.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carers, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix F - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.