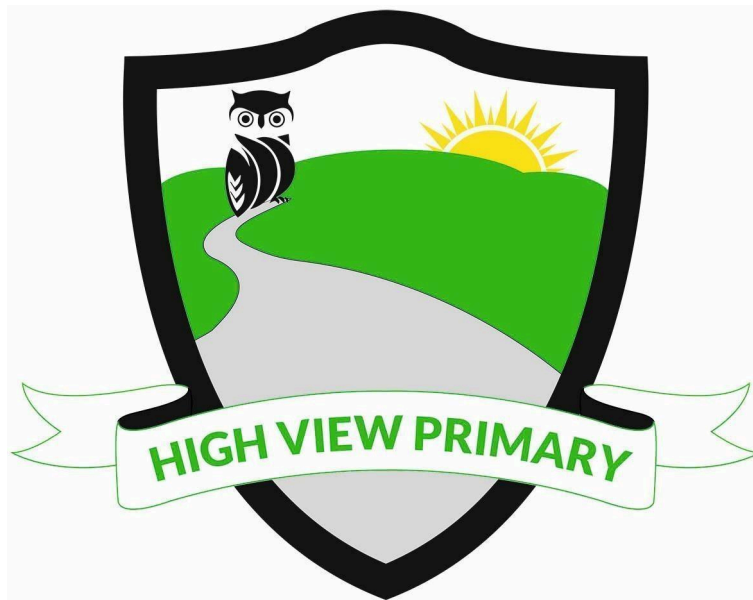


---

# High View Primary School



**Opportunities to Thrive**

# **Online Safety & Acceptable User Policy**

**Summer Term 2024**

Date for review: Summer Term 2026

## Contents

What is this Policy?	4
How will this Policy be communicated?	4
Overview	5
Scope and Definitions	5
Aims	5
Further Help and Support	6
Current Online Safeguarding Trends	6
Roles and responsibilities	7
Education and Curriculum	7
Handling Online-Safety Concerns and Incidents	8
Unacceptable Use	9
Use of Technology - Pupils	10
Access to ICT Facilities	10
Search and Deletion	10
Unacceptable Use of ICT and the Internet Outside of School - Pupils	12
Use of Technology - Parents/Carers	12
Access to ICT Facilities and Materials	12
Communicating with or about the School Online	12
Communicating with Parents/Carers about the Pupil Activity	13
Use of Technology - Staff (Including Governors, Volunteers and Contractors)	13
Access to the School ICT Facilities and Materials	13
Use of Phones and Email	13
Personal Use	14
Personal Social Media Accounts	14
Remote Access	14
School Social Media Accounts	14
Trips / Events Away from School	15

Monitoring and Filtering of the School Network and use of ICT Facilities	15
Data Protection and Cyber Security	16
Digital Images and Video	16
School Website	17

## **Appendices**

Appendix 1 - Annex A - Roles and Responsibilities Outlined	18
Appendix 2 - Staff Acceptable Use Statement	25
Appendix 3 - Children Acceptable Use Statement	29

## What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2023](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)

## How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs are issued to the whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review or pupils move from KS1 to KS2.

- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

## Overview

### Scope and definitions

This policy applies to all members of the High View Primary School community (including teaching and support staff, supply teachers, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

### Aims

At High View, Online Safety is integrated throughout our curriculum to support the teaching and learning requirements to aid the building of essential life skills. Each topic will be catered and refined to benefit the needs of our children. Online safety is a part of our children's daily lives and teaches them how to conduct themselves both on and offline.

The aims of Online safety at High View are to:

- Promote the safety, awareness, knowledge and understanding to all pupils
- Encourage pupils to understand how to use and enjoy the internet safely
- Teach pupils about relationships online
- Provide pupils with a toolkit for understanding and managing online information
- Provide pupils with the opportunities to consider issues which may affect their own lives and/or the lives of others
- Help pupils develop feelings of self-respect, confidence and empathy
- Provide a framework in which sensitive discussions can take place
- Promote safety in forming and maintaining relationships
- Allow pupils to experience how they can be represented online in a safe environment
- Teach pupils to understand what constitutes a safe and healthy lifestyle
- Provide pupils with a toolkit to create balance in an ever-growing technical world.

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology
- Set clear guidelines for the responsible use of technology for the whole school community
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.
- Have effective, robust filtering and monitoring strategies that meet the safeguarding needs of our school

This policy aims to:

- Set out expectations for all High View Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

### **Further Help and Support**

Please report any concerns to the school's DSL or DDSL details of which can be located in the school office.

Beyond this, [reporting.lgfl.net](https://www.lgfl.net/reporting) has a list of curated links to external support and helplines for both pupils and staff. Including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via [safetraining.lgfl.net](https://www.lgfl.net/safetraining)

### **Current Online Safeguarding Trends**

Below are some of the current trends which have affected the wellbeing and safeguarding of our students:

- sending unkind messages on social media and group chats

- playing online games with older age restrictions such as 'Fortnite'
- having profiles on social media accounts such as TikTok and sharing content of themselves and others
- parents sharing concerns about the amount of time spent on a device and how to manage this
- being influenced by Youtubers

We work collaboratively to ensure any concerns about pupils' online usage and safety are robustly dealt with. Should you have any concerns or have any further questions, please get in contact.

## **Roles and responsibilities**

We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time. All staff have a key role to play in safeguarding children and feeding back on any potential issues.

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school. In addition, to ensure all pupils access technologies safely and responsibly, both at home and in school, and ensure personal knowledge and understanding is up to date to aid the support of the children's safety. The DSL is responsible for ensuring effective filtering and monitoring practices.

All members of the community should immediately report any concerns or inappropriate behaviour to the DSL or DDSL to protect staff, pupils, families and the reputation of the school. Where appropriate, this should then be recorded on CPOMs (in line with behaviour and anti-bullying policy).

All members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff, which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex (Appendix 1).

## **Education and curriculum**

The following subjects have the clearest online safety links (see the relevant role descriptors for more information):

- Computing
- PSHE curriculum (see PSHE policy), which includes Relationships and Sex Education (RSE) as well as Health and Citizenship

As previously stated, online safety is integrated throughout the curriculum. It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/keystage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote

teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow this framework more closely in its key areas.

## Handling online-safety concerns and incidents

Online Safety is an integral part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship) and it is vital all members of the High View community are robust when handling concerns.

### 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 scams

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Protection Policy - Safeguarding
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF) or the NSPCC Whistleblowing Helpline.

Any suspected online risk or infringement should be reported to the designated safeguarding lead immediately.



Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

### **Unacceptable use**

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
  - During assessments, including internal and external assessments, and coursework
  - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or a member of the Senior Leadership Team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities, and act accordingly with behaviour, safeguarding or disciplinary procedures.

## Use of technology - Pupils

### Access to ICT facilities

- Chromebooks and Interactive boards are available to pupils to use during lessons to complete the main task or so an adaptation under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- All pupils are provided with a google classroom account and email which they should always use when accessing any school device
- All pupils can access learning platforms and applications to support home learning, each pupil will be given an individual log in, and should not share passwords
- All devices pupils have access to will be monitored to ensure pupils are safeguarded at all times.
- Pupils in years 5 and 6 are allowed to bring mobile phones in for use beforehand after school, but must be handed to the class teacher on arrival and will be kept in the classroom until returned at the end of the day - we accept no responsibility for the lost or damage of technology pupils choose to bring into school.
- Pupils and parents understand and are made aware of where the use of tracking smartwatches which can also receive messages are not to be worn at school.

### Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has 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

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- 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, and how and where the search will happen, and give them the opportunity to ask questions about it

- Seek the pupil's co-operation (if the pupil refuses to cooperate, you will proceed according to our behaviour policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in our Behaviour Policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a 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 a device, the staff member should only do so if they reasonably suspect that the data has been, 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 headteacher or 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 whether there is a good reason to erase data or files from a device, staff members will consider whether 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 is 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
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [searching, screening and confiscation](#) and the UK Council for Internet Safety (UKCIS) et al.'s 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 et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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

## **Unacceptable use of ICT and the internet outside of school - pupils**

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

We ask all pupils to sign the acceptable user agreement (appendix 3a for KS1 and appendix 3b for KS2)

## **Use of Technology - Parents/Carers**

### **Access to ICT facilities and materials**

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Parents are asked to leave their phones in their pockets and turned off when they are on site. When at school events, please refer to the Digital images and video section of this document on page.

### **Communicating with or about the school online**

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

All parents will be given the class email address for the class their child/ren is in.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents/carers to sign the pupil agreement to agree to support their child.

## **Communicating with parents/carers about pupil activity**

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

## **Use of Technology - Staff (including governors, volunteers, and contractors)**

### **Access to school ICT facilities and materials**

The school's network manager, Cygnet, the Headteacher, the school's business manager and DSL will manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the headteacher or DSL.

### **Use of phones and email**

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission should be sought from the HT.

The school provides each member of staff with an email address, and class teachers will also be provided with a delegated class email.

This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable of all school devices.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

### **Personal use**

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher or DSL may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of class emails to protect themselves online and avoid compromising their professional integrity.

### **Personal social media accounts**

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Social media checks are made as part of our recruitment process.

### **Remote access**

We allow staff to access the school's ICT facilities and materials remotely, via Google Drive.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

### **School social media accounts**

The school has an official Twitter account, managed by the Leadership Team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They will also not use personal mobile phones or cameras to take pictures of pupils.

We monitor emails and internet use on the school IT system.

### **Trips / events away from school**

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

### **Monitoring and filtering of the school network and use of ICT facilities**

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network.

This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Keys pressed on school chromebooks
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

As a school we:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

At this High View, the internet connection is provided by LGfL. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. We use Classroom.cloud to monitor the usage of school chromebooks both inside and outside of school, to ensure we safeguard our pupils at all times.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards

- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL or DDSL.

### **Data protection and cybersecurity**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policy, which can be found here ([Data Protection Policy](#)) It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE that also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection:

USO sign on for LGfL services, Sophos Anti-Virus, CloudReady/NeverWare and Lgfl HomeProtect (on the chromebooks used for remote learning).

### **Digital images and video**

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the school publications (for example, the school newsletter)
- For use in paper-based school marketing
- For online prospectus or websites



- For social media
- For Twitter
- For school photos
- For external publications/company's (for example afterschool clubs, theatre workshops)
- For local media
- For use in Department of Education Publications
- For photos to be circulated to other parents (school productions, residential trips)

Whenever a photo or video is taken/made, the member of staff taking it will check the latest permissions on the pupil database (SIMS) before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At High View, no member of staff will ever use their personal phone to capture photos or videos of pupils, without the explicit permission from the Headteacher.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy. Staff and parents are reminded periodically about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

### **School website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value.

The DfE has determined information which must be available on a school website and the Senior Leadership Team of the school ensures that these requirements are met.

- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

A copy of this policy is available on our school website

## Outlines and Responsibilities

### Headteacher

#### Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

### Designated Safeguarding Lead / Online Safety Lead

Keeping Children Safe in Education (KCSIE) makes clear that “the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety).” The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

#### Key responsibilities:

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead** responsibility should not be delegated”

- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see [safetraining.lgfl.net](https://www.gov.uk/guidance/safetraining-lgfl-net) and [prevent.lgfl.net](https://www.gov.uk/guidance/prevent-lgfl-net)
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox/
- Ensure the 2021 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex A
  - it would also be advisable for all staff to be aware of Annex C (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation

## Governing Body, led by Online Safety / Safeguarding Link Governor

### Key responsibilities (quotes are taken from Keeping Children Safe in Education 2020)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#)
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards (see [coronavirus.lgfl.net/safeguarding](https://www.gov.uk/guidance/coronavirus-lgfl-net/safeguarding) for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- "Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including

online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”

- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice from the local three safeguarding partners integrated, aligned and considered as part of the overarching safeguarding approach.”
- “Ensure appropriate filters and appropriate monitoring systems are in place; be careful that ‘overblocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding”. LGfL’s appropriate filtering submission is [here](#)
- “Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology.”

## All staff

### Key responsibilities:

- Recognise that in **RSHE** online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone’s job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school’s main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum.
- Whenever overseeing the use of technology in school or for home or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.

- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- **Prepare and check all online source and resources before using**
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

## **PSHE / RSHE Lead**

### **Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Work closely with the Computing lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

## **Computing Lead and Online Safety Lead**

### **Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum within computing lessons
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

## Subject leaders

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

## Network Manager/technician

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

## Data Protection Officer (DPO) –

### Key responsibilities:

- NB – this document is not for general data-protection guidance; GDPR information on the relationship between the school and LGfL can be found at [gdpr.lgfl.net](https://gdpr.lgfl.net);
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:  
*"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to*

**process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) *When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children.”*

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

## LGfL TRUSTnet Nominated contacts –

### Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at [gdpr.lgfl.net](http://gdpr.lgfl.net)

## Volunteers and contractors

### Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a volunteer or contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

## Pupils

### Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Treat any **home learning** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen

- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

## **Parents/carers**

### **Key responsibilities:**

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

## **External groups including parent associations**

### **Key responsibilities:**

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers



**High View Primary School – ACCEPTABLE USE STATEMENT (STAFF)**

To ensure that all members of staff are fully aware of their professional responsibilities when using information and when communicating with pupils, they are asked to sign this Acceptable Use Statement. For further information and clarification, staff should consult the school's Computing Policy and Data Protection Policy.

The computer system is owned by the school and is made available to staff to enhance their professional activities, including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system. The school may exercise its right to monitor the use of the information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's systems may be taking place, or being used for criminal purposes or for the storage of inappropriate or unlawful text, imagery or sound.

All staff (including supply and temporary) requiring Internet access should sign a copy of this Acceptable Use Statement and return it to the School Business Manager

- I understand that it is a criminal offence to use the school ICT system or service for a purpose not agreed by the school and the Headteacher or Governing Board.
- I understand and address the 4 key categories of risk: Content, contact, conduct and commerce
- I will only use the school's email / Internet / Intranet / Google Classrooms and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Board
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises (only if encrypted to AES 256 standard or higher) or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software without permission of the Headteacher.
- I will only open email attachments from sources I know to be safe.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored, logged and made available, on request, to the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not “friend” a pupil on my personal social networking accounts, blog or other services.
- I will support and promote the school’s Computing and E-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will report any incidents of concern regarding a pupil’s safety or information security to a DSL and Headteacher.
- Access to the internet and school server should only be made via the authorised account and password, which should not be made available to any other person.
- It is the responsibility of staff members to make the Computing Lead aware of occasions when passwords cease to become private.
- Staff should ensure that high levels of data-protection are adhered to at all times. This means locking computers whilst leaving the room.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden. Permission should be granted from the Headteacher before bringing in electrical and ICT equipment from home (Where appropriate this must be PAT tested).
- Users are responsible for all emails sent and for contacts made that may result in email being received.
- Use for personal financial gain, gambling, political purposes, online shopping or advertising is forbidden.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

- I will report any incidents relating to abuse or harassment directed at me via any form of communication such as email, social networking or other systems to the Headteacher.
- I am aware my school will monitor my usage on school devices.

I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Any breaches in the operation of the requirements laid out in this Acceptable Use Statement will result in the Disciplinary Policy being invoked.

Full name: .....

Signed:.....Date: .....



## High View Primary School – ACCEPTABLE USE STATEMENT (EYFS and KS1)

### To help me stay safe online

My name is \_\_\_\_\_

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone
12. My actions are **MONITORED** on school computers

**I have discussed this with an adult and understood this agreement. If I break this agreement I realise that there may be a consequence.**

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

As the **parent/carer** of a High View pupil, I agree to support my child with the above statements at home.

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_



## High View Primary School – ACCEPTABLE USE STATEMENT (KS2)

**This agreement will keep me safe and help me to be fair to others**

**My name is \_\_\_\_\_**

1. ***I learn online*** – I use the school's internet, resources and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords! I do not ask others for their passwords.
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

~~~~~

**I have read and understood this agreement. If I break this agreement I realise that there may be a consequence.**

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

As the **parent/carers** of a High View pupil, I agree to support my child with the above statements at home.

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_