# Higham Ferrers Nursery and Infant School

**‘Together, we enjoy learning in a happy, caring and friendly environment’**

# *COMPUTING POLICY*

*(INCLUDING ACCEPTABLE USE, ONLINE SAFETY, INTERNET ACCESS, USE OF MOBILE PHONES AND WEBSITE)*

**This Policy was agreed by the Full Governing Body in Autumn (2023)**

**It will be reviewed in Summer (2025)**

Signed: H. R. Robbins

(Chair of Governors)

## 01. INTRODUCTION

At Higham Ferrers Nursery and Infant School, we appreciate how computing is changing the lives of everyone. Through teaching computing and online safety we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. Computing skills are a major factor in enabling children to be the confident, creative and independent learners of today and citizens of the future.

## 02. AIMS

Our aim is to produce learners who are confident and effective users of IT. We are striving to achieve this by:

- Enabling teachers to become confident in the implementation of the computing National Curriculum including online safety.
- Providing good quality up to date hardware, software and technical support.
- Developing a curriculum that will help all children to use computing with purpose and enjoyment, help them to develop the necessary skills to become autonomous users and to utilise computing in all subject areas, and help them to evaluate the benefits of computing and its impact on society.
- Meeting the requirements of the National Curriculum and helping all children to achieve the highest possible standards of achievements by implementing the skills taught through cross curricular approaches in our connected curriculum.
- Celebrating success in the use of computing including online safety through displays, computing portfolio on server.
- Using IT to develop partnerships beyond the school and with other schools.
- Networking all the computers in the school.
- Exploring attitudes towards computing and its value to individuals and society in general for example, to learn about issues of security, confidentiality and safety.

## 03. TEACHING AND LEARNING STYLE

3.1 As the aims of computing are to equip children with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We teach specific computing skills and plan for opportunities throughout the curriculum for the children to implement those skills.

3.2 We recognise that all classes have children with widely differing computing experiences and abilities. This is especially true when some children have access to IT equipment at home, while others do not. Through careful observation and assessment we are able to plan for the varied skills the children have in each class, providing suitable learning opportunities for all children by matching the challenge of the task to the ability and experience of the child.

## 04. CURRICULUM PLANNING

The school uses the National curriculum for computing, alongside the 'Kapow' scheme as the basis for its curriculum planning.

We carry out the planning for computing in three phases (long-term, medium-term and short-term). The long-term plan maps the computing topics that the children study in each term during each key stage. Our long-term IT plan shows how teaching units are distributed across the year groups and how these fit together to ensure progression.

Our medium-term plans give details of the unit of work to be taught for each term. They identify the key skills for each unit.

Individual computing skills lessons are taken straight from the 'Kapow' scheme of work and these plans list the specific learning intentions of each lesson. In KS1 each class teacher is responsible for the delivery of these skill-based lessons. These skills are implemented through cross curricular links. The opportunities to apply the computing skills that are taught should be clearly marked on all planning throughout the whole curriculum.

The computing subject leader monitors the planning and feeds back to year group leaders. The class teacher is responsible for annotating the short-term plans from every subject to show how computing is being used in a cross curricular way.

## 05. EARLY YEARS FOUNDATION STAGE

Early Years foundation staff through discussions with parents at the beginning of the year find out what IT experiences the children have. This enables teachers to pitch the work at the right level and challenge those with more experience. The computing subject leader uses this baseline data from to gain a picture of the children's awareness of computing. Computing in the Foundation Stage classes is taught as an integral part of the topic work covered during the year. Using the Early Years Foundation Stage Framework teachers ensure that IT is delivered through all aspects of the children's work to the objectives set out in the Early Learning Goals (ELGs) which underpin the curriculum planning for children aged three to five. Progress and attainment in computing is monitored and measured four times a year on the school's tracking system – O Track.

The children have the opportunity to use I-Pads, interactive whiteboards and programmable toys, and engage in role play with day to day equipment (for example toy washing machines, toasters and telephones.)

Apps on the I-Pads are also used to support children with phonics, letter formation, number and shape recognition.

## 06. CONTRIBUTION OF IT TO OTHER CURRICULUM AREAS

6.1 IT contributes to teaching and learning in all curriculum areas. For example, graphics work links in closely with work in art, and work using databases supports work in mathematics, while apps and the Internet prove very useful for research. Computing enables children to present their information and conclusions in various ways. Children should always be taught to use the internet safely throughout any lesson.

6.2 PERSONAL, SOCIAL AND HEALTH EDUCATION, (PSHE) AND CITIZENSHIP

Computing contributes to the teaching of PSHE and citizenship as children learn to work together in a collaborative manner. Through the discussion of moral issues related to electronic communication, children develop a view about the use and misuse of IT, and they also gain a knowledge and understanding of the interdependence of people around the world.

## 07. TEACHING COMPUTING TO CHILDREN WITH SPECIAL NEEDS AND DISABILITIES

Computing forms part of our school curriculum policy to provide a broad and balanced education for all children. We provide learning opportunities that are matched to the needs of children with learning difficulties. In some instances, the use of IT has a considerable impact on the quality of work that children produce; it increases their confidence and motivation.

## 08. ASSESSMENT AND RECORDING

8.1 Teachers assess children's work in computing by making informal judgements as they observe them during lessons. Pupils' progress is closely monitored by the class teacher and at the end of each term; each pupil will be levelled for the strand of computing which has been studied. All assessments are entered onto O-Track. When appropriate pupils save work into their folders on the server.

8.2 The IT subject leader views samples of the children's work from 3 levels of achievement from specific strands. This demonstrates the expected level of achievement in IT for each age group in the school.

## 09. RESOURCES

9.1 There are netbooks and tablets and I-Pad minis for the children to use. Each classroom has a PC (in the process of being upgraded) and one full-sized I-Pad.

There is a computer in the Staffroom for all staff to access. This computer is linked to a colour printer and a photocopier.

Each classroom has an interactive whiteboard. All classes have smartboard panels. Every computer in the school is linked to the internet and also has the McAfee VirusScan program. We keep resources for IT, including software, in classrooms and the staffroom. We have boxes of programmable toys which are shared across the school. Each teacher has a laptop which can be used for planning and assessment.

9.2 The school has a variety of 2Simple software installed on their computers. We also have a Volume Purchasing Program with Apple which enables us to bulk buy apps at a reduced rate.

9.3 The school uses the cloud based system ‘google drive’ for email and also for the sharing and storage of information. Information can be stored and selectively shared via this system.

## 10. MONITORING AND REVIEW

The monitoring of the standards of the children’s work and of the quality of teaching in IT is the responsibility of the IT subject leader and the Senior Leadership Team. The IT subject leader is also responsible for supporting colleagues in the teaching of IT, for keeping them informed about current developments in the subject and for providing a strategic lead and direction for the subject in the school. The IT subject leader has regular meetings with the headteacher to review the IT subject improvement plan (SIP). Ideally the IT subject leader meets with the IT link Governor throughout the year.

In addition to this, the IT subject leader;

- Writes (and actions) a subject improvement plan, which is shared with the Head teacher and Governors annually;
- Liaises with the link Governor;
- Attends regular cluster and county IT meetings;
- Reviews the quality and appropriateness of hardware and software in school regularly.

## HIGHAM FERRERS NURSERY AND INFANT SCHOOL ONLINE SAFETY

## 11. INTRODUCTION TO ONLINE SAFETY

It is the duty of all staff at our school to ensure that every child in our care is safe, and the same principles apply to the ‘virtual’ or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not always age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy, supported by our Acceptable Use Policies (AUP; see appendices) for staff, governors, visitors and pupils, is to protect the interests and safety of our whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following Higham Ferrers Nursery and Infant School policies: Safeguarding and Child Protection, Whistleblowing, Staff Code of Conduct, Awareness and Prevention of Child Sexual Exploitation (CSE), Behaviour, Anti-Bullying and Data Protection.

Both this policy and the Acceptable Use Policies (Appendix one) for all staff, governors, visitors and pupils are inclusive of both fixed and mobile internet, technologies provided by our school (such as PCs, laptops, whiteboards, tablet, digital video and camera equipment, etc) and technologies owned by staff.

IT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world, all at the touch of a button. At present, a wide-variety of internet based technologies are used extensively by young people in both the home and school environment.

Whilst this technology has many benefits for our school community, it is recognised that clear procedures for appropriate use and education for all staff, governors, visitors and pupils about online behaviours, age restrictions and potential risks, is crucial.

## 12. THE TECHNOLOGIES

IT in the 21st Century has an all-encompassing role within the lives of our children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets
- Voice controlled technologies such as ‘Alexa’

## 13. WHOLE SCHOOL APPROACH TO IT

Creating a safe IT learning environment includes three main elements at our school:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive Online safety education programme for our pupils, staff and parents.

## 14. STAFF RESPONSIBILITIES

Online safety is recognised as an essential aspect of strategic leadership in our school and our Head Teacher, with the support of governors, aims to embed safe practices into the culture of our school. Our Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are responsible for ensuring that confidentiality and safeguarding is always the highest priority. Staff are aware that no personal or sensitive information should be shared at any time, during meetings with other professionals only relevant and appropriate information is shared for the correct purposes.
All staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis. All visitors also receive an online safety briefing on arrival at our school by way of our Safeguarding Leaflet. The overall responsibility for online safety is the responsibility of the DSL but all staff have the responsibility to ensure the online safety of all children in school.

Our Information Technology (IT) subject leader ensures that they liaise with our Designated Safeguarding Leads in order to keep up to date with all Online safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP) and training delivered by our external Online safety trainer. Our school's IT subject leader ensures that our Head, Senior Management Team and Governors are updated as necessary.

## 15. STAFF AWARENESS

- All staff receive regular information and training on Online safety issues through a number of means:
  - ❖ Annual Online safety staff training
  - ❖ Weekly briefing (which always includes safeguarding issues)
  - ❖ In-house safeguarding updates and training
  - ❖ GDPR Awareness Training

- New staff receive information on our school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of Online safety and know what to do in the event of misuse of technology by any member of our school community.
- All staff incorporate Online safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- If there are Online safety concerns staff know that a Cause for Concern (C4C) form must be completed as soon as an incident occurs. These forms can be located on any of our five Safeguarding Stations, located around our school. Once completed, the C4C form must be placed in a sealed envelope and reported/passed directly to any member of our school's designated safeguarding leads. Concerns can also be uploaded onto 'My Concern'.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online safety procedures. These behaviours are summarised in our AUPs which staff sign to say they have read and understood, at the beginning of each new school year, or if they are new to our school.

## 16. THE INTERNET

- At Higham Ferrers Nursery and Infant School we use TalkStraight “filtered” Internet Service, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the internet through our school’s fixed and mobile internet technology.
- Staff should email school-related information using their **@hfi.education** address and not personal accounts. Staff and Governors have been asked not to access GMail accounts via the App on a device as this prevents the user from being able to log out of the account. Use the browser route and ensure account is fully logged out when finished.
- Staff will preview any websites before recommending them to pupils.
- The CEOP Report Abuse button is available on our school website.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to any of the Designated Safeguarding Lead(s) detailing the device and username. TalkStraight can then be informed.
- Staff are aware that school based email and internet activity will be regularly monitored and can be explored further if required. A monitoring report sent from the ISP (TalkStraight) is analysed by the Head Teacher and/or the IT Technician.
- Staff are to be aware of phishing emails from unusual addresses and not click on links or open emails unless the source is known.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then this will be reported to TalkStraight so that further access to the site can be blocked.
- Pupils are expected not to use any rude or offensive language in their searches on the internet.
- Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following our school’s behaviour policy.
- These Online safety rules are summarised in our Home/School Agreement which pupils are asked to sign with the support of their parents, ensuring that they are aware of expectations. Copies of the agreement are distributed to parents to ensure that key messages are reinforced at home.

## 17. PASSWORDS

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters. Staff are asked to refrain from using numbers, family names or dates of birth in passwords as these days, this type are increasingly easy to decode.)
- All passwords should be changed when asked to do so, or every 3 months (Staff and Governors).
- If passwords are written down then they must never be kept with a portable device (laptop), must be kept away from computers, and ideally kept in a locked cupboard/drawer.
- Passwords should not be shared.

## 18. MOBILE TECHNOLOGY (LAPTOPS, I-PADS, NETBOOKS, ETC)

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- The bit-locker code should never be kept with laptops or in laptop bags.
- Staff should only use the laptop which is allocated to them and will be asked to sign an updated laptop agreement in light of GDPR legislation.
- Staff and Governors will be allowed to use their own devices, such as phones and tablets, providing they are securely protected by a complex password or pincode. Multi-factor verification must be in use when registering a new device. No photos, data or pupil information is to be stored on these devices and staff will be subject to checks on these devices if they have been used.
- Laptops (and PCs) should always be locked if left unattended.
- Staff should not upload any programmes to their school laptop. This should only be completed by our in-house IT technician.
- Staff are aware that their school laptop based email and internet activity will be regularly monitored and can be explored further if required.
- Mobile technology for pupil use, such as I-Pads and netbooks, are stored in a locked cupboard. They must be returned here when asked to by the IT coordinator. Access is available via our school IT subject leader.
- Mobile Technology assigned to a member of staff as part of their role and responsibility have a passcode or device lock so unauthorised people cannot access the content.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times only, out of sight of children and kept on silent. See Appendix A for use of smart watches in school. All bags containing any mobile devices should always be stored in classroom cupboards out of children’s reach.
- Video Conferencing for remote learning must be agreed by the headteacher and staff must ensure they follow guidance in appendix 3 alongside the online safety policy.

## 19. DATA STORAGE

- **Data will be stored in line with GDPR requirements.**
- Staff are expected to save all data relating to their work onto Google drive and on their Laptop if they have been assigned one or onto the school server.
- If staff need to use removable media, it must be in the form of an encrypted memory stick provided by our school or via Google drive. Staff must not use a non-encrypted memory stick or hard drive to store data.
- Laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school or on Google drive or T-Drive
- Staff must only take off site information that they are authorised to and only when it is necessary and required in order to fulfil their role. If they are unsure, they should speak to one of our Designated Safeguarding Lead(s).

## 20. SOCIAL NETWORKING SITES

- Use such sites with extreme caution.
- Be aware of the nature of what is being published on-line in relation to professional position. Do not publish any information online (as a member of staff at Higham Ferrers Nursery and Infant School) which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- All staff roles in our school require a high degree of professionalism and confidentiality.
- Any communications or content published by any members of staff that causes damage to our School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which our School and Local Authority Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.
- Any communications made in a professional capacity through social media must not either knowingly or recklessly:
    - place a child or young person at risk of harm;
    - bring our School into disrepute;
    - breach confidentiality;
    - breach copyright;

- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - ❖ making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - ❖ using social media to bully another individual; or
  - ❖ posting images that are discriminatory or offensive or links to such content.

**Our School reserves the right to monitor staff internet usage on a daily basis, any abnormal or suspicious activity will generate an alert sent to the Headteacher, SBM or IT lead, that will be addressed immediately. Our School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.**

## 21. DIGITAL IMAGES

- Use only digital cameras and video cameras provided by our school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.
- If images are taken on mobile phones for specific purposes then it must be in school with the permission of the Headteacher/DSL and phones must be checked prior to leaving the building.
- Ensure you are aware of the children whose parents/guardians have **not** given permission for their child's image to be used in school. An up to date list is kept in the school office.
- When using children's images for any school activity, they should not be identified by their full name.
- Do not store school based photographs on in-house devices (I-Pads) for long periods of time.
- Regularly download them onto Server-T under the appropriate class or year group number.
- Ensure that you regularly delete photos from google drive or the server. Photos should not be kept for more than a couple of years.

**Members of staff who breach our acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.**

## 22. PROVIDING A COMPREHENSIVE ONLINE SAFETY EDUCATION TO PUPILS AND PARENTS

- All staff working with children must share a collective responsibility to provide Online safety education to pupils and to promote Online safety in their own actions.
- Formally, an Online safety education is provided by the objectives contained in the IT unit plans for every area of work for each year group. Even if Online safety is not relevant to the area of IT being taught, it is important to have this as a 'constant' in the IT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows Online safety issues to be addressed as and when they arise.
- The IT subject leader will lead an assembly each term on Online safety, highlighting relevant Online safety issues and promoting safe use of technologies.
- All classes will follow a themed week at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.
- Information will be constantly drip fed via lessons and assemblies.
- When children use school computers, staff should make sure that they are fully aware of the Online safety guidelines outlined in this policy.
- Parents/carers will be invited to attend an Online safety awareness workshop once per year, run by our school's IT subject leader in conjunction with pupils and an external Online safety trainer.
- Children will have the opportunity to educate parents through assemblies and classroom activities on an annual basis.

## 23. MAINTAINING THE SECURITY OF THE SCHOOL IT NETWORK

TalkStraight maintains the security of our school network and is responsible for ensuring that virus protection is up to date at all times. However it is also the responsibility of IT users to uphold the security and integrity of the network.
The school also employs an independent IT technician who is DBS checked and GDPR compliant who supports in the maintenance of the system and all linked devices.

## 24. OUR WEBSITE

Higham Ferrers Nursery and Infant School values the contribution that a website can make to the life and role of our school in a modern society. Our website has three important roles:

- To promote our school
- To provide information to prospective parents/carers, teachers and the wider community
- To act as a communication channel between our teachers, parents/carers, pupils and school management

### 24.1 WEBSITE STRUCTURE

Our school website is http://www.highamferrersinfants.org.uk . The site is hosted on TalkStraight servers and is provided by the Joomla CMS Open Source platform. There are two main sections to the site: -

- The front end published site, which is available to anyone in the world with Internet access
- The private back end site, which is available only to authorised members of the school community

Access to the private back end is controlled by username and password. Joomla allows the Site Administrator to create an unlimited number of users that can access and add content to the site. Users are teachers and authorised administration staff. User accounts are only created with the approval of the Head Teacher.

### 24.2 SAFEGUARDS

The safety of children, families and other users who appear or are referred to on the published site is of paramount importance. The school will ensure that no pupil can be identified or contacted either via or as a result of using the school website. The following best practice procedures have been put in place by our school to ensure the safeguarding of our children on our website:

- Right click protection is applied to all photographs posted onto our website to prevent them being copied.
- Permission will be obtained from parents or carers before any pupil's image is used.
- Permission will be obtained from parents or carers before publishing the work of any pupil. Only first names and year group will be used to identify the work.
- No close up pictures of individual children will be available online – only group photographs with two or more children.
- A general written statement will be placed against the photograph so that individual children are unable to be singled out.
- Any images of children will not be directly labelled with their names.
- Names and photographs of children will only be used if permission has been given by parents/carers. (See appendix 1)
- Adults' names will be published as their title and last name e.g. Mr. Smith. Children's names will be published as their first name only e.g. Jacob, or if required, first name and year group e.g. Jacob P4.
- Children will only be shown in photos where they are suitably dressed.
- Personal details of children or staff such as home addresses, telephone numbers, personal e-mail addresses, etc, will **NEVER BE** released via our website.
- Links to external websites will be checked thoroughly before inclusion on the school website. The sites will be checked for the suitability of their content for their intended audience.
- Any text written by pupils will be reviewed before inclusion to ensure that no personal details are accidentally included that could lead to the identification of the pupil e.g. membership of after school clubs.
- All written work will be reviewed to ensure that it is in no way defamatory.
- Written work will be checked to ensure (as far as possible) that no copyright or intellectual property rights are infringed.
- All written material will be checked for its suitability for its intended audience.
- Parents/Carers reserve the right to withdraw permission for their child's image or first name to be used on our website.

### 24.3 ACCESS AND APPROVAL

Content on the school website is controlled by secure access. There are 2 roles: Super Administrators and Administrators. All material submitted to the site is initially given a status of 'Unpublished' and cannot not appear on the live site until promoted from 'Unpublished' to 'Published' status by an authorised person with the Administrator role.

*Administrators* are allowed to submit new pages and upload photographs via the backend for approval prior to publication. *Administrators* are allowed to edit their own content and also other *Administrator's* content. They are allowed to promote 'Unpublished' content to 'Published' status. *Administrators* may also demote 'Published' content to 'Unpublished'.

*Super Administrators* have full access to the Joomla environment for the purposes of maintaining the software and the underlying technical environment. This includes tasks such as user administration and software maintenance and upgrade. Super Administrators have the ability to publish content but will not publish materials to the site unless expressly authorised by the Head Teacher.

**Privacy**

Adults have the right to refuse permission to publish their image on the site.

Parents have the right to refuse permission for their child's work and/or image to be published on the site.

Those wishing to exercise this right should express their wishes in writing to the Head Teacher, clearly stating whether they object to work, images, or both being published. Parents will be notified of this right by publication of this policy on an annual basis with an acknowledgement receipt attached.

### 24.4 MONITORING

An *Administrator* will check material before it is uploaded or published to ensure that it is suitable and complies with the record of objections held by the Head Teacher and with copyright laws (as far as is possible). Any persons named on a web page can ask for their details to be removed.

New pages will be tested for errors immediately after installation.

The web pages will be regularly reviewed for accuracy and will be updated as required. This review will occur at least annually. It will be the responsibility of an Administrator, school management, staff or authorised agents to ensure this happens.

### 24.5 MAINTENANCE AND EDITING

Written instructions and manuals will be available and maintained by the Administrator covering how to update the website. At least two people should have the knowledge to maintain and edit the site, and they must pass on their knowledge to a successor at the end of a term of office.

### 24.6 EMAIL

The site uses a single email address to notify a nominated email account that content is awaiting action (for example that a website visitor needs information). This address is generic (i.e. not identifiable to a single person) and monitored by those users assigned the role of administrator. It is used solely for the purpose of communicating to administrators that content requires action and not for any other purpose. The generic office email should be used when contacting parents.

Class specific emails will be used in the case of school closures and online learning. If staff members or governors are using an email app to access emails, multi factor verification is required to ensure that the device is secure. Devices with an email app to access emails will require device password protection, alongside the multi factor email verification, to ensure that emails are secure and cannot be viewed by those without the appropriate permission.

### 24.7 COMPLAINTS PROCEDURE

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to Online safety then they will be considered and prompt action will be taken. Complaints should be addressed to the Head Teacher who will undertake an immediate investigation and liaise with those members directly involved. Incidents of Online safety concern will be recorded using a Cause for Concern proforma and reported to our school's Designated Safeguarding Lead(s), in accordance with our school's Safeguarding and Child Protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

## 25. MONITORING

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any IT equipment owned or leased by the school at any time. In order to keep children safe when using school IT equipment, we use Talk Straight filtered internet service as an internet filter. This is monitored by the DSL/headteacher, IT technician, online safety lead and School Business Manager who receive a daily report from Talk Straight which provides any safeguarding alerts so that they can be investigated immediately.

## 26. ROLE OF GOVERNORS

- Support appropriate safeguarding procedures by allocating resources effectively;
- Ensure school buildings and premises support effective delivery of our website to our parents/carers and community;
- Monitor the website regularly with the website administrator in light of safeguarding;
- Monitor processes which lead to effective safeguarding of our website;
- Ensure that staff development and performance management support appropriate levels of professional conduct;
- Review effectiveness of our website through school self-review processes and parent/carer questionnaires.
- To read, accept and sign the Acceptable Use Policy as detailed in this policy.

## 27. ROLE OF PARENTS

- Parents have a fundamental role in supporting their child's learning.
- Parents have a responsibility to ensure that they supervise their children when using the internet to ensure that they use age appropriate software and programmes. fulfil the requirements set out in our Home/School Agreement

## 28. APPENDIX 1 – ACCEPTABLE USE POLICY AT HIGHAM FERRERS NURSERY AND INFANT SCHOOL

IT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from Online safety incidents and promote a safe E-learning environment for pupils.

- I will only use our school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will create a strong and different password for all devices allocated to me.
- I will change passwords in line with school policy.
- I will not keep my bit-locker key or passwords written down anywhere near my PC or laptop.
- I will not disclose my password to anybody else.
- When accessing school emails, or any other sensitive information relating to Higham Ferrers Nursery and Infant School, I will ensure that it is conducted on a device that has the appropriate security measures (anti-virus, firewall, encryption) and one which will be locked down when I am away from the device and I will log off each of the sites after use. I will access my school Gmail account via a browser and not via the Gmail application.
- I will only access emails when children are not present.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will ensure that my private wider online presence (Facebook, Instagram etc) are compatible with my professional role. My social media accounts will be kept private.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not add school pupils or parents, past or present, as friends, unless known to me as a friend or relative prior to my appointment.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If I bring my own personal devices into school, these will only be used during non-contact time without pupils if for personal use. If for school use then I understand they must not be used to store pupil data, photos or information regarding staff members and the device must be password protected. Smart watches used in school must not have the ability to take photos and will not be accessed/responded to when in class with the children present.
- Any phones must be kept in a bag in a cupboard and not left on a shelf or in view of children.
- I will report any Online safety concerns to the designated safeguarding officer immediately using the Online safety Record of Concern.

- Mobile phones will be out of sight in classroom or staffroom cupboards and switched to silent.
- I will support the school's Online safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
- When using digital methods of communication (emails, chat apps, video conferencing), no sensitive or confidential information will be shared at any time in line with GDPR requirements, to maintain appropriate safeguards for children, families and staff.
- Where DSLs may need to share confidential information with appropriate staff for safeguarding purposes, the subject line must read CONFIDENTIAL and such emails should only be read before or after the school day.

I understand the procedures and agree to follow them with immediate effect.

Print Name: _______________________
Signed: ____________________________ Date: __________________

## 29. APPENDIX 2 – DATA BREACHES AT HIGHAM FERRERS NURSERY AND INFANT SCHOOL

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-
***Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.***

Staff should only save sensitive data in the following secure formats:-

- On the encrypted USB memory stick provided
- On an encrypted laptop provided
- On Google drive

This ensures that no legal action can be taken for lost data.

Staff are encouraged to hold all of their data on their school laptop that has a built-in level of encryption. If this is not possible and they have not been allocated a laptop they are encouraged to save all of the data onto their encrypted memory stick or onto Google drive.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the Head Teacher without delay. It is imperative that you do not share or write down your password. You may add a question prompt reminder when first accessing your memory stick, which can be used if you have forgotten your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format as detailed above. Sensitive data should not be sent via email to external agencies, third party agencies or those not employed by our school unless it is encrypted/password protected.
Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

I understand the procedures and agree to follow them with immediate effect.

Name ________________________ Signed________________________________

Date _________________________

## 30. APPENDIX 3 – VIDEO CONFERENCING

### Purpose

These aims are to ensure that:

- Pupils, staff and parents understand how video calling can support children
- Staff, parents, careers and external partners know how to stay safe during video conferencing calls
- Staff, parents/careers and external partners are complying with Safeguarding requirements, GDPR requirements and Video conferencing etiquette when using video conferencing

### Currently Supported Platforms

The only video conferencing platforms authorised for use at the school are:

- Zoom
- Microsoft Teams
- Google

### Scope

Video calls maybe authorised by the school to enable the following activities.

- Supporting SEND/identified pupils
- Emotional support/mental health and wellbeing
- Motivation and engagement
- Communication with parents
- Safeguarding
- Operational running of the school: staff meetings, planning for teaching & curriculum, HR, finance, health & safety, Governors meetings.

### Roles and Responsibilities:

**Computing Lead**

The Computing Lead is responsible for:

- Ensuring that all staff are aware of this policy and understand their role in its implementation
- Ensuring that adequate training is provided for staff to support the effective implementation of this policy
- Implementing clear and effective strategies to ensure staff, parents, careers and external partners are kept safe online

- Keeping this policy and the use of video conferencing under regular review, at least annually
- Notifying parents about the use of video conferencing and make them aware that the school policy is available on the website for parents and careers to view. This will reflect the behaviour the school expects from staff, parents, careers and external partners when video conferencing takes place and should be made available to all parties.

These responsibilities will be overseen by the Head Teacher and SLT.

**Staff**

Staff are responsible for:

- Ensuring that they follow this policy, are aware of current guidance and procedures relating to online learning, and have received appropriate training before utilising video conferencing.
- This policy is intended for use in conjunction with the following School policies:

i) Child Protection and Safeguarding,
ii) GDPR policies
iii) Computing
iv) Staff Code of Conduct

- Following the School's safeguarding procedures will ensure that no information not relevant to discussions is shared.
- Ensuring their remote account is kept separate from their personal accounts, using or setting up a school account for any online platform used, and checking the privacy settings.

**Parents/ Careers/ External Partners**

We expect parents to support the School by:

- Ensuring they are aware of the behaviour the school expects from parents/careers when video conferencing takes place.
- Contact the school if they have any feedback or concerns about the use of video conferencing.

## Following the School's Procedure

**Video calls**

- Parents/Careers/Colleagues/External partnerships will be informed of the platforms that staff are to use. This will be posted on our school newsletter, email or communicated via phone calls.
- Video calls between staff and other parties will take place via Google

software, Teams or Zoom.

- Teachers will notify Parents/Careers/Colleagues/External partners in advance of any video calls taking place and provide with a copy of the **<u>Video Conferencing Etiquette</u>**
- Details on how to join into the video meeting will be sent prior to the start time
- Staff will use virtual waiting rooms. This will enable the school to check who they are before allowing entry.
- Everyone must be on time to the video meeting.
- Screen sharing will be limited, this will ensure that others do not take control of the screen and prevent them from sharing random content.
- File transfer will be disabled.
- The environment that the video call is taken place will be carefully considered and does not breech any Safeguarding or GDPR requirements.
- To ensure that safeguarding of the children, families and staff is always considered. No sensitive, confidential or personal information will be shared.

**Parent/Careers/External partnership video calls**

- Parent/careers/external partnership calls will take place via Zoom/MicrosoftTeams/Google and the teacher will be located in school.
- Parent/careers/external partners will be informed of the video call via letter or email, including details of how to access the meeting and general meeting etiquette.
- For meetings, the staff member will send the parent/careers/external partners the link (via their work email address) to join the meeting.
- Staff will ensure that they are accessing the School's MIS (SIMS) for up-to-date contact details for parents.
- Parents who do not want to meet via video call have the option to disable their camera on the call or can be offered a telephone call instead.
- Only information relevant to the topic of the meeting will be discussed.

**Staff video calls (including Governors)**

- Video calls between staff will take place via Zoom/MicrosoftTeams/Google using their work accounts.
- Meetings will be scheduled via Zoom/MicrosoftTeams/Google
- Dress code - professional attire (ref. code of conduct).
- Location of meeting should be considered (e.g. avoid areas with background noise, nothing inappropriate in the background, no GDPR breaches, photographs of staff children, personal possession, confidentiality of personal life and not in the bedroom)

### Video Conferencing Rules for Staff

- Staff should only make video conferences via a school device using their school account.
- Staff will use Zoom/MicrosoftTeams/Google
- Staff should turn off file transfer
- No person within the video call will share any personal information e.g. personal telephone number, email accounts, Facebook and other social media links. Staff should never use personal social media accounts as a 'short cut' to communicate with anyone.
- Sensitive and confidential information outside of the appropriate topic conversations will not be discussed.
- Ensure staff members work against a neutral background. Staff should present themselves as they would if they were giving a face-to-face meeting and dress appropriately.
- All staff should be aware of the School's child protection and safeguarding policy and procedures. Ensure that staff members can contact the Designated Safeguarding Lead any concerns about a child

### Video conferencing etiquette: Expectations of Participants

- Everyone must respect others within the video call and no inappropriate language or actions will be used – all school rules and values must be followed
- Be aware that all those who join the meetings will be able to hear anything you share, so please contact school separately if you wish to discuss an issue specific to you
- Staff and other members of the meetings must wear suitable clothing
- Please do not make any kind of recording of the meeting in any way, including taking screenshots or photographs of the screen
- Everyone must show their face/have their camera on to enter the video call so we can see who has joined us. Set up the camera so we can see the participant and, ideally, no- one else in the household
- Consider the position of your device (pc, phone or tablet) when you are joining the meeting, ensure there is nothing inappropriate in the background and that background noise is limited.
- Video calls should not take place in a bedroom or bathroom.
- Try to use a quiet communal space
- Do not reveal passwords or personal information to anyone

- Do not share the invitation, link or passcode with anyone else
- Do not share any school content on social media platforms including screenshots and photos of online sessions.