

Farley Hill Primary School



Computing Online Safety Policy

Governing Body Responsibility: Learning and Impact Committee	Approved: November 2024
	Next Review: November 2025

1 Aim

Our school aims to:

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

The 4 key categories of risk

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

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

2 Legislation and guidance

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

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- Relationship Education
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

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

The policy also takes into account the National Curriculum computing programmes of study.

3 Roles and Responsibilities

3.1 Governors

Governors are responsible for the approval of the Computing and Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In

fulfilling this responsibility, the governing body may choose to appoint an online safety governor and establish an online safety committee with appropriate representation. Governors will require/undertake the following regular activities:

- All governors will ensure that they have read and understood this policy
- Agree and adhere to the terms of the school's Code of Conduct policy
- Meet with the online Co-ordinator.
- Monitor online safety incident logs.
- Report to relevant governor committees.
- Keep up to date with school online safety matters
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 Headteacher

The Headteacher is responsible for ensuring the safety, including online safety, of members of the school community. The day to day responsibility for online may be delegated to the Online Safety co-ordinator, ICT Subject Leader or another appropriate member of staff. However, the Headteacher will ensure the following:

- Staff with online responsibilities receive suitable and regular training enabling them to carry out their online roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious online allegation being made against a member of staff.

3.3 Online Safety Co-ordinator

The online Co-ordinator has day to day responsibility for online issues and takes a leading role in establishing and reviewing the school online Policy and associated documents. The Online Safety Co-ordinator will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide materials and advice for integrating online safety within schemes of work and check that online is taught on a regular basis.
- Liaise with the local authority.
- Liaise with the school's technical staff (external ICT provider).
- Ensure that online incidents are reported and logged and used to inform future online developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

3.4 External ICT Provider

The External ICT Provider and, where appropriate, the Online Safety Co-ordinator and ICT lead, will, in cooperation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. The filtering policy and its implementation is not the sole responsibility of any single person.
- The ICT infrastructure is secure and protected from misuse or malicious attack and updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- The school meets the online technical requirements outlined in any relevant local authority online policy/guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy, in which passwords are regularly changed.
- Online technical information is kept up to date, applied as necessary and passed on to others where relevant.
- Use of the network, learning platform and pupil e-mail is regularly monitored and any misuse/attempted misuse reported to the Online Safety Co-ordinator or designated person for investigation and action.
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media.
- Provide secure access to the school network from home where necessary using VPN or equivalent technologies.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and Volunteers

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

- Maintaining an understanding of current online safety matters and the school Online Safety Policy and practices.
- Implementing this policy consistently
 - They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement, annually actioned by SBM. They ensure that pupils understand and follow the school's online and Acceptable Use Policies.
- They report and log any suspected misuse or problem to the Online Safety Co-ordinator and DSL for investigation and action in line with this policy
- Digital communications with pupils (e-mail/learning platform/voice) should be on a professional level and only carried out using approved school systems.
- Online issues are embedded in all aspects of the curriculum and other school activities.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.

- They are aware of online issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Child Protection Officer/Designated Safeguarding Lead (CPO/DSL)

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

The DSL should be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

3.7 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk. SLT should be informed where school policies may require updating.

3.8 Parents

Parents are expected to:

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

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Learning Platform. This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

3.9 Visitors and Members of the community

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

4 Training

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

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

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

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

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

5 Reviewing, Reporting and Sanctions

5.1 Review

- This policy will be reviewed and updated annually, or sooner if necessary.
- The school will audit ICT provision to establish if the online Policy is adequate and that its implementation is effective.

5.2 Acceptable Use Agreements

- All users of the school computers will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils where It is signed when pupils join the school.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.

5.3 Reporting

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and the NetSmart Code of Practice (acceptable internet use) for EYFS/KS1 and KS2. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.

5.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

5.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

6 *Educating pupils about online safety*

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools

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

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

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

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

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

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

7 **Communications & Communication Technologies**

7.1 **Mobile phones and personal handheld devices**

- Pupils will not be allowed to bring mobile phones or items with SMART Technology e.g SMART watches with phone or video/recording capabilities or internet access into school unless prior arrangements are made with the school. Mobile phones are kept in the office during the school day.
- Where mobile phones or SMART Technology are allowed in school they may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images will be viewed as serious and fully investigated.

- If necessary, searches will be made for mobile phones/SMART technology if staff have become aware that children may have them in school (and have not handed the phones into the school office) or have them during an off-site visit e.g., school residential. Phones will be confiscated if this is the case and returned at an appropriate time to the child or parent.
- Pupils will not be allowed to bring in games devices and other electronic equipment, particularly those which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- If Staff have to use their own phones in an emergency, they would withhold their number using 141 and delete the contact number once used.
- Staff mobile devices should normally be switched off or on silent during the times that children are present.
- Mobile phones belonging to helpers and visitors are stored in the office whilst they are in school.
- No device in any of the school buildings should contain any content that is inappropriate or illegal. The school has filtering and monitoring processes in place.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.2 E-mail and messaging

- Staff will be informed that the use of school e-mail accounts will be monitored.
- Staff may access personal web-based e-mail accounts, or other social media apps, from school on their own mobile devices or technology, but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene. The school has filtering and monitoring processes in place.
- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.
- Information of a sensitive nature should not be sent by e-mail.

7.3 Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction, e.g., Facebook, Twitter, WhatsApp, i-Messaging, Tik Tok, Snapchat, blogs, online gaming, YouTube, Skype, Second Life, etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity. Staff **MUST NOT** use personal social networking sites to contact parents or pupils. In extenuating circumstances such as during a school trip, staff mobile phones may need to be used to contact parents directly in the case of an emergency involving their child. (see section 7.1)
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.

- The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within a school learning platform is both acceptable and to be encouraged.

Refer to Appendix 1 for Farley Hill's Social Networking Procedure

7.4 Social Media

Social media has been identified as an important tool in the sharing of extreme material and extremist groups are actively using social media to inform, share propaganda, radicalise and recruit for their cause. Social media safeguarding is an important element of protecting young people from extremist narratives. "PREVENT" can play an active part in the process.

Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Refer to Preventing Extremism and Radicalisation Policy

To report any online terrorist related material go to www.gov.uk/report-terrorism

7.5 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's online Guidelines. These should be posted near to the computer systems.
- *Pupils will receive guidance in responsible and safe use on a regular basis*
- *All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.*
- *Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.*
- *We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.*

7.6 Digital and video images

Parents, staff and pupils may record images of pupils at school under the following conditions:

- Parental permission must be obtained for the taking and use of digital and video images of pupils.
- Images should not be used on school learning platforms and/or websites or publicity without express permission from the parent, and where such permission has been obtained individual pupils should not be identifiable by name.
- All staff digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- The use of staff personal devices is not acceptable unless agreed with a member of SLT in advance and for a specific purpose.
- Parents, Staff and Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images should not be distributed beyond either the school or the immediate family and friends of the pupil's family and not shared on social media.
- Images of pupils must be stored securely and deleted when no longer required.
- No images of pupils should be recorded in toilets or wash areas, whilst pupils are getting changed or in the medical room. The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g., how to wash hands). In this case the line manager must be informed before this activity is undertaken.

7.7 Learning platform and/or website

- The school website should include the school address, school email, telephone number including any emergency contact details.
- The school website should be used to provide information and guidance to parents concerning policies and practice.
- Staff or pupils' home information should not be published.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g., via Creative Commons licensing.

7.8 Home Learning

The school has the capability to use video conferencing technology to allow all pupils to access learning from home and communicate with their teacher, if necessary, e.g., during lockdown.

The school has created a specific set of guidelines to manage such an event. Parents must have read the Code of Conduct and agreed to and signed a copy of the Contract of Use before being able to access the video conferencing facility.

Please see attached Appendix 3 for the Remote Learning policy

8 Infrastructure and Security

8.1 Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School ICT technical staff and external ICT provider may monitor and record the activity of users on the school ICT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the External ICT Provider.
- Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- The 'Administrator' passwords for the school ICT system, used by the External ICT Provider are also available to the Head Teacher and ICT Subject Leader and must be stored securely in school.
- SBM must remove staff and pupils from all systems e.g., Learning Platform.

8.2 Passwords

All staff are provided with an individual password. Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the learning platform and/or secure areas of the website.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- Once a computer has been used, users must remember to log off so that others cannot access their information.
- Users leaving a computer temporarily should lock the screen (Windows key + L).
- Passwords should be changed at regular intervals. The school may choose to enforce this requirement through the use of Windows Password Policy where passwords are changed for example every three months.
- In the event that a password becomes insecure then it should be changed immediately.

8.3 Filtering and Monitoring

The filtering system blocks internet access to harmful sites and inappropriate content. It should not: unreasonably impact teaching and learning, school administration or restrict students from learning how to access and manage risk themselves.

The school maintains and supports a managed filtering and monitoring service provided by external provider (RM), the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL). The provision is reviewed annually but regular checks are completed every term to ensure systems are working effectively and safeguarding needs are being met. All checks on the system will be recorded.

The Head Teacher and Computing Governor are responsible for the filtering and monitoring, with support from the SBM and IT Support Team.

The Senior Leadership team are responsible for:

- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of our provision
- Overseeing reports

They are also responsible for making sure that all staff:

- Understand their role
- Are appropriately trained
- Follow policies, processes and procedures
- Act on reports and concerns

The DSL has responsibility for safeguarding and online safety, which could include overseeing and acting on:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

The IT service Providers (RM) have technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems

The IT service provider works with the Senior Leadership team and DSL to:

- Procure systems
- Identify risk
- Carry out reviews and carry out checks

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- They witness or suspect unsuitable material has been accessed
- They can access unsuitable material
- They are teaching topics which could create unusual activity on the filtering logs
- There is failure in the software or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- They notice abbreviations or misspellings that allow access to restriction material

A variety of monitoring strategies are used to minimise safeguarding risks on internet connected devices and include:

- Physically monitoring of staff watching screens of users
- Pupil awareness of what is appropriate or not to view
- Network monitoring using log files of internet traffic and web access
- Individual device monitoring through software or third-party services

Changes to network filtering should be approved by the ICT Subject Leader and the External ICT Provider.

Any filtering issues should be reported immediately to the ISP and/or SEGfL.

8.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
- The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only dependable sources should be used.
- Staff should have access to and be able to use security software to remove adware and malware.

8.5 Staff laptops/devices

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

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
- Laptops/devices should never be left in a parked car, even in the boot.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.
- *Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)*
- *Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device*
- *Making sure the device locks if left inactive for a period of time*
- *Installing anti-virus and anti-spyware software*
- *Keeping operating systems up to date – always install the latest updates*

Staff members must not use the device in any way which would violate the school's Code of Conduct policy.

8.6 Personal and sensitive data

- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.

- Sensitive data is any data which links a pupil's name to a particular item of information and:
 - must be encrypted on laptops/devices, memory sticks, CDs and any other removable media;
 - should not be e-mailed between staff;
 - should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
- Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.
- There are clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

8.7 Loading/installing software

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the External ICT Provider or ICT Subject Leader, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

8.8 Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
- No data should be stored on the C drive of any curriculum computer as it is liable to be deleted and all data lost, if the PC would require reimaging/rebuilding. This is due to the backup process.
- Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The school should also define a whole school ICT disaster recovery plan which would take effect when severe disturbance to the schools ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

Refer to Appendix 2 for Farley Hill's IT System Procedure

9 Online Education

9.1 Learning and teaching for pupils

- Children receive information linked to online safety through explicit teaching and as an ongoing focus across the curriculum
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key online messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities. Potential risks posed by online activity, including cyberbullying and the use of Apps such as 'WhatsApp' will be discussed as part of their learning.

Rules for the use of computers should be displayed in all rooms and displayed next to fixed site computers. (SMART)

9.2 Staff training

- Staff will be kept up to date through regular online training.
- Staff should always act as good role models in their use of ICT, the internet and mobile devices.

10 Cyber-bullying

10.1 Definition

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

10.2 Preventing and addressing cyber-bullying

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

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

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

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

10.2 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images **(without looking at these images)** or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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

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

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

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

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

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

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

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

11 Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaint's procedure
- ICT and internet acceptable use policy

12 Monitoring arrangements

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

This policy will be reviewed every year by the [Head teacher and Computing Lead]. At every review, the policy will be shared with the governing board.

Appendix 1 Social Networking

Introduction

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is important to ensure that we balance this with our duties to our school community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide a balance to support innovation whilst providing a framework of good practice. They apply to all school stakeholders, including employees, governors, students and pupils. For the purpose of this policy, these groups are referred to collectively as "School Representatives".

Purpose

The purpose of this policy is to ensure that:

- Farley Hill Primary School, its leaders and governors are not exposed to legal risks;
- the reputation of Farley Hill Primary School, staff and governors are not adversely affected;
- all children are safeguarded;
- any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of Farley Hill Primary School.

Scope

The requirements of this policy apply to all uses of social networking applications which are used for any school or local authority related purpose and regardless of whether the applications are hosted corporately or not. They must also be considered where school representatives are contributing in an official capacity to social networking applications provided by external organisations. Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, media sharing services, "Microblogging" applications. Examples include Twitter, Facebook, MSN, You Tube. Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All School Representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Local Authority Equality and Safeguarding policies.

Use of Social Networking Sites in Work Time

Use of social networking sites in work time for personal use only is not permitted, unless permission has been given by the Headteacher.

Terms of Use

School representatives must adhere to the following Terms of Use which apply to all uses of social networking applications. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Farley Hill Primary School 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.

Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring that school into disrepute
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff
- Must not breach the school's disciplinary or equalities policy
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a "friend" to share information with
- Employees should not identify themselves as representatives of the school
- References should not be made to any staff member, pupil, parent or school activity/event unless prior permission has been obtained and agreed with the Headteacher
- Staff should be aware that if their out of work activity causes potential embarrassment for the employer or detrimentally affects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Appendix 2 IT System Procedure

IT System Access Rights

The Headteacher and School Business Manager will have full administrator rights on the administrative system.

The Computing Leader and IT Company will have full access rights to all curriculum areas and the Learning Platform.

Other staff will be granted limited rights with the approval of the system administrators according to their needs.

Licences

The School Business Manager is responsible for office software licences. The Computing Leader is responsible for curriculum software licences.

Back Up Arrangements

All data is automatically backed up remotely by our IT Company on a daily basis.

Passwords

Each staff member is responsible for choosing secure and appropriate passwords to protect sensitive data and is responsible for changing them regularly.

Data Management

All staff entering data on the School system will be made aware of the requirements of the Data Protection and Freedom of Information Acts and the School's FOI Publication Scheme and Records Management Policy.

Anti Virus Protection Software:

Panda

Our IT Company ensure appropriate anti-virus software is in place and reviewed regularly.

Hardware and Software Maintenance

All hardware will be entered on to the School Inventory and broken or obsolete equipment should be disposed of according to School Policy.

System Issues: These will be referred to our IT Provider.

Appendix 3 Remote Learning



User guidelines for video conferencing into pupils' homes **(Code of Conduct)**

Aim: What to expect during a video conference class?

The aim at Farley Hill Primary School is to maintain our community approach. In times where our children and staff are not at school and home based. We want to provide an opportunity for our staff and children to stay in contact with each other. We will use video conference technology to provide a secure meeting place for each class to meet two or three times a day so the teachers can maintain some form of communication and outline the timetable for the day with children and to pick up any challenges the children may face with their online learning.

Pupils and Parents:

- Please be aware that everything is shown on camera and heard through the microphone!
- Please be aware of the background your child is seated in front of. Keep it simple and plain. No bedrooms.
- Do not sit your child in front of a window. This will cast a dark shadow.
- The area your child is seated in needs to be as quiet as possible so they can hear the audio clearly and see the image on the screen. There should be no other distractions.
- If possible, use a surface that allows paperwork next to the computer/device.
- Please make sure your child is appropriately dressed (smartly to attend the video conference).
- Positive language and the school behaviour policy is to be used at all times.
- The class will be recorded for monitoring and safeguarding.
- We do not allow virtual backgrounds (this drains bandwidth).
- The children must log in with their first names, if they are not, they will not be admitted into the room.
- The room will be locked at the start time, and pupils are to arrive 10 minutes before the start and wait to be admitted into the room.
- Late comers will not be admitted.
- If you lose internet connection during the Video Conferencing you will unfortunately not be allowed back into the room because it will be locked.
- If you lose your Identification code/Password access details to the classroom, please contact your class teacher 24 hours before your class is due to start and no later.



Contract of Use

Agreement for Video Conference Classes

We are asking for your support and understanding in undertaking this new way of teaching and learning with video conference technology whilst your child is at home.

Please note that the school is not responsible for the quality of your video conference connection. The quality relies heavily on your internet connection at home and the device you are using.

1. Please abide to the code of conduct.
2. Any parent or child sharing the Identification code or Password with another adult or child will be removed from video conferencing classes.
3. Other than by the teacher, no videos, recording or photos of the video conferences will be allowed.
4. No images/recordings of the video conference are to be shared on social media.
5. The children must follow the behaviour policy of the school even though they are at home.
6. There will be zero tolerance against any verbal/ visual abuse towards staff or other pupils during the video conference.
7. Should you lose the Identification code or Password please contact the class teacher by email, giving 24 hr before the video conference. Less than 24 hr notice may mean that you are not able to connect into the lesson.
8. By signing this agreement, you are giving permission to the school to record your child during the video conference, for safeguarding and monitoring purposes only.
9. The school will do its best to give at least 24hr notice if there is a reason that class may need to cancel.
10. Parents are not to engage in conversation with teachers during the lesson – this can be done over email. This lesson is for the children only
11. When signing into zoom children must type use their first names to log in with
12. The video on the webcam must be switched on at all times.
13. There are to be no use of virtual backgrounds.
14. No other child or adult is to be seen on the screen. Child only.
15. The meeting will be locked at a set time after which any late comers will not be allowed into the meeting.

If any of the above rules are broken, you will be removed from all future video conferences immediately.

I have read, understood and agree to follow the Farley Hill Contract of Use Agreement for Video Conference Classes.

Parent Full Name: _____

Child Full Name: _____

Class: _____

Signed: _____

Date: _____