LONG MEADOW SCHOOL

ICT, ONLINE, E-SAFETY AND ACCEPTABLE USE POLICY

Date of last review:	June 2023
Date of next review:	June 2026
Type of policy:	Non-Statutory
Frequency of review:	Every 3 years
Governor committee:	Governing Body

Contents

1 Aims and scope of the policy

1.1 Aims of the policy

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies, including those on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

For online safety, it aims to:

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

1.2 Scope of the policy

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors both in and out of school.
The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

Breaches of this policy may be dealt with under our behaviour and staff code of conduct policies. The school will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2 Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and it
refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Protecting children from radicalisation.
- 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 Definitions

- **ICT facilities:** all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the school's ICT service

- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

- **E-safety**: a part of safeguarding which means protecting children from risk on websites and apps, including social media. Risk can be categorised into four areas:

- **Content** – being exposed to illegal, inappropriate or harmful material which may include pornography, fake news, racist or offensive views, radical or extremist views, misogyny, underage apps or online gaming.
- **Contact** – being subjected to harmful online interactions with other users, e.g. bullying, grooming, sexual harassment, aggressive advertising or pressure to spend money.
- **Conduct** – behaving in a way that causes the likelihood of harm, e.g. making, sending or receiving explicit images – consensually or non-consensually or bullying others.
- **Commerce** – online gambling, inappropriate advertisement, phishing or financial scams.

4 Roles and responsibilities

Responsibility for ICT, acceptable use and e-safety lies with the headteacher. All adults working with children using any IT device are responsible for not only keeping them safe, but also educating them to the challenges faced in the online world. All adults working in the school are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Role	Key Responsibilities
Headteacher	● To take overall responsibility for e-safety provision ● To take overall responsibility for data and data security ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (Currently Protex, backed by Eqiinet, approved by DfE) ● To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles ● To be aware of procedures to be followed in the event of a serious e-safety incident. ● To receive regular monitoring reports from the e-safety coordinator ● To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures ● Ensures staff will model safe and responsible behaviour in their own use of technology during lessons. ● Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights; ● Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling ● Monitor reports of e-safety issues on CPOMS
E-safety Coordinator	● To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy ● To promote an awareness and commitment to e-safeguarding throughout the school community ● To ensure that e-safety education is embedded across the curriculum ● To liaises with school ICT technical staff ● To communicate regularly with SLT and the governing body to discuss current issues and incidents ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident ● To ensure that the CPOMS e-safety incident log is kept up to date ● To facilitate training and advice for all staff ● To liaise with the Local Authority and relevant agencies ● To remain regularly updated in e-safety issues and legislation
Computing and ICT Link Governor	● To ensure that the school follows all current e-safety advice to keep the children and staff safe

Role	Key Responsibilities
	● To approve the e-safety Policy and review the effectiveness of the policy. ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities
Computing Curriculum Leader	● To oversee the delivery of the e-safety element of the Computing curriculum ● To liaise with the e-safety coordinator regularly
Network Manager	● To report any e-safety related issues that arises, to the e-safety coordinator. ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy. ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) ● To ensure the security of the school ICT system ● To ensure that access controls exist to protect personal and sensitive information held on school-owned devices • To ensure web filtering is applied and updated on a regular basis • To keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To check that the use of the *remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator ● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. ● To keep up-to-date documentation of the school's e-security and technical procedures
School Data Manager	● To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	● To embed e-safety issues in all aspects of the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	● To read, understand and help promote the school's e-safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Policy ● To report any suspected misuse or problem to the using an e-safety incident form – available in the staff area on the network ● To maintain an awareness of current e-safety issues and guidance ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never

Role	Key Responsibilities
	through personal mechanisms, e.g. email, text, mobile phones and private messaging ● Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
Pupils	● To read, understand, sign and adhere to the Pupil Internet Agreement ● To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the use of mobile phones, digital cameras and hand-held devices. ● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home ● To help the school in the creation/ review of e-safety policies
Parents/carers	● To support the school in promoting e-safety and endorse the 'Pupil Internet Agreement' ● To consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

5 Unacceptable use

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

Unacceptable use of the school's ICT facilities includes:

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

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

5.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. If this occurs, the headteacher will inform the chair of governers.

5.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and the staff code of conduct.

6 Staff (including governors, volunteers, and contractors)

6.1 Access to school ICT facilities and materials

The school's network manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.
Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the network manager.

6.2 Use of phones and email

The school provides each member of staff with an email address.
This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).
All work-related business should be conducted using the email address the school has provided.

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

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

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

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

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
If staff send an email in error that contains the personal information of another person, they must inform the school business manager immediately and follow our data breach procedure.

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

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use. These are the school phone used for trips and the learning mentor's phone.

6.3 **Personal use**

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

Personal use is permitted provided that such use:

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

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

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

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy.

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

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

6.4 **Personal social media accounts**

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. See the social netowrking policy for further information.

6.5 **Remote access**

We allow staff to access the school's ICT facilities and materials remotely using OpenVPN and an E2BN config file. It is managed by the network manager.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the network manager may require against importing viruses or compromising system security.

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

6.6 **School social media accounts**

The school has an official Twitter account. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account. Each member of staff may also have their own Twitter account.
The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

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

6.8 **Protection on the school's network**

- The school computing network has a firewall and web-filtering system in place, known as Protex. Should any material of an inappropriate nature appear on a device in school, details of the web address must be maintained and the school's internet service provider, E2BN, can be informed so that it blocked in future.

- Protex is used by many Local Authorities to provide a compliant web filtering service for hundreds of schools in the UK. E2BN applies Internet Watch Foundation Child Sexual Abuse block lists and Home Office "Prevent" lists. It is compliant with DFE guidelines. Further details can be found here: http://blog.e2bn.org/wp-content/uploads/2016/09/Appropriate-filtering-response-E2BN.pdf

The effectiveness of any filtering and monitoring will be regularly reviewed.
Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and ICT manager, as appropriate.
The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

6.9 **Staff using work devices outside school**

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use,

Work devices must be used solely for work activities.

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

6.10 How the school will respond to issues of misuse

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 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.

6.11 Training

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

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

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

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

Training will also help staff:

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

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

The DSLs 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.

6.12 How do staff raise concerns?

Staff should raise their concerns by reporting them via CPOMS to the Designated Safeguarding Leads. An online safety incident is a safeguarding issue so it should be treated like any other safeguarding concern or incident. Staff should act and do so quickly, following the school's behaviour and child protection policies. If a child has been harmed, is in immediate danger, or is at risk of harm, the police or children's social care will be contacted where necessary.

7 Pupils

7.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Additional equipment, such as iPads and Chromebooks, may also only be used under the supervision of staff
- Some pupils may be provided with an individual Chromebook or iPad to use within the school.
- Year 6 pupils may bring in a mobile phone which must be kept in the teacher's cupboard when in school

7.2 Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

- Relationships and sex education and health education in secondary 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

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

7.3 **How e-safety is taught**

E-safety is taught as part of the computing curriculum and 'Being Safe Online' needs to be referred to in every computing lesson. E-safety is also taught in PSHE lessons with reference to staying safe and cyber-bullying. It is an essential part of 'circle time' discussions. All Key Stage 2 classrooms have the 'SMART' Childnet International poster on display giving advice on E-safety behaviour and all Key Stage 1 and Early Years classrooms have a Smartie the Penguin poster on display. School assemblies are also used to provide information to the children at key points in the year.

7.4 **Pupil e-safety curriculum**

The curriculum covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music/video files – without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for various reasons;
- to understand the impact of their conduct online e.g. cyberbullying or sending/receiving explicit images and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline.

7.5 **Cyber-bullying**

7.5.1 Definition

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

7.5.2 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. 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 (see section 11 for more detail).

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

In relation to a specific incident of cyber-bullying, the 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 Designated Safeguarding Lead will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.6 **Examining electronic devices**

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

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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

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

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

If inappropriate material is found on the device, it is up to the headteacher or designated safeguarding lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

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

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

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

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

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

7.7 Search and deletion

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

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

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or a designated safeguarding lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (If a pupil refuses, follow the behaviour policy)

The authorised staff member should:

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

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

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

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

7.7 Unacceptable use of ICT and the internet outside of school

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

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community

- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

7.8 How do pupils raise concerns?

Pupils will be taught to raise concerns when they feel uncomfortable on line at anytime, either at home or in school. They will be shown how to turn the screen off so that the information is retained but cannot be seen by other children. They will then be taught how to tell their parent, carer or teacher immediately. In situations where a child has been made uncomfortable by the actions of another online user, they need to be taught how to report this via CEOP or the NSPCC. The 'CEOP Report' button is on the front page of the school website.

8 Parents

8.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.
However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.
Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.
Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels. Parents must follow the Parent Code of Conduct.

8.3 Communicating with parents about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.
When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks is shared.

In particular, staff will let parents know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.
Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

8.4 **Educating parents about online safety**

The school will raise parents' awareness of internet safety in weekly newsletters or other communications home, and in information via our website. Information for parents on the content of the annual 'Internet Safety Day' will be provided. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

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

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

8.5 **How do parents raise concerns?**

In the first instance, parents and carers should report their concerns to the class teacher. If the information is of a particularly sensitive nature, parents and carers may wish to speak directly to the headteacher or a Designated Safeguarding Lead.

9 Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.
Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

9.1 **Passwords**

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their

passwords and accounts, and for setting permissions for accounts and files they control.
Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.
Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

9.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.
Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
Any personal devices using the school's network must all be configured in this way.

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

9.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
These access rights are managed by the headteacher.
Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the headteacher immediately.
Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

9.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the network manager.

10 Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data every night to an on-site Network Attached Storage (NAS) box and offsite to MFM-IT cloud storage so they can be stored off the school premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the network manager
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

- Develop, review and test an incident response plan including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.

- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

11 Internet access

The school's wireless internet connection is secure.

11.1 **Pupils**

WiFi is available on devices where children must be supervised to be used. Security settings and filtering mentioned previously is on all devices.

11.2 **Parents and visitors**

Parents and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.
The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

12 Monitoring and review

The headteacher monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.
The governing board is responsible for reviewing and approving this policy.
The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 3 years by the computing subject lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will reflect the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13 Links with other policies

This policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- Social networking
- Remote education
- Mobile phone

Appendix 1: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and headteacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: ● Use them without asking a teacher first, or without a teacher in the room ● Use them to break school rules ● Go on any social networking sites (unless my teacher said I could as part of a lesson) or chat rooms ● Open any attachments in emails, or click any links in emails, without checking with a teacher first ● Use mean or rude language when talking to other people online or in emails ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Share my password with others or log in as someone else ● Share inappropriate images of myself or others I understand that the school will check the websites I visit and how I use the school's computers and equipment. I will tell a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. We expect our pupils to follow SMART rules on e-safety S – Safe – Keep safe by not sharing personal information, name, address, phone number, password, photos, school name to people you don't know on-line M – Meeting – Do not meet up anyone you know online without your parents being there too A – Accepting – Do not accept messages, files, requests, pictures from people you don't know R – Reliable – Information may not always be true. People may not be who they seem T – Tell – Tell someone if you feel uncomfortable or worried about something that has happened on-line I understand that there will be consequences if I don't follow the rules. This may mean I will be denied access to internet resources.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during school time lessons, at clubs or other activities organised by the school, without a teacher's permission
- I will hand it into my teacher when I arrive at school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the there will be consequences if I don't follow the rules. This may mean I will be denied access to internet resources.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Our official Twitter pages ● Email/text for parents (for school announcements and information) Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: ● Follow the Parent Code of Conduct and the Home-School Communication Policy ● Be respectful towards members of staff, and the school, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: ● Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way ● Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident ● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**