

Online safety policy

Hillary Primary School



Approved by:
The Governing
Body

Date: 08.07.20

Last reviewed on:
24.6.20

Next review due
by:

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	2
4. Educating pupils about online safety	4
5. Educating parents about online safety	5
6. Online bullying	5
7. Acceptable use of the internet in school	7
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school	7
10. How the school will respond to issues of misuse	7
11. Training	8
12. Monitoring arrangements	9

13. Links with other policies.....	9
14. Online safety Policy Covid 19 addendum.....	9
Pupil Acceptable Use Policy Agreement -Early Years	12
Pupil Acceptable Use Policy Agreement - Key Stage 1.....	13
Pupil Acceptable Use Policy - KS2	14
Acceptable use policy for staff	15

1. Aims

Our school 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department'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 online 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 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Sana Ejaz.

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Head teacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding lead (DDSL) are set out in our child protection and safeguarding policy.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, Computing Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on ischool, as with all safeguarding incidents and dealt with appropriately in line with this policy
- Ensuring that any incidents of online 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

This list is not intended to be exhaustive.

3.4 The ICT technician (LA ICT)

The ICT technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged using 'ischools' or reported to an appropriate person and dealt with appropriately in line with this policy
- Ensuring that any incidents of online-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 this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on 'ischools' and dealt with appropriately in line with this policy
- Ensuring that any incidents of online-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 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 (appendix 1)

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

- What are the issues, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

3.7 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 2).

4. Educating pupils about online safety

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

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
- Online Safety in the curriculum

A programme of training in online safety will be taught to children across the school from Nursery to Year 6.

Early Years Foundation Stage and Key Stage 1

At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult. Children will be taught key skills of logging on, how to complete safe searches and what is appropriate and inappropriate.

Lower Key Stage 2

Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc.). They will be shown how to develop a responsible attitude towards searching the Internet and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2

Children will now be encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the Internet using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and safer schools app. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings or parent workshops.

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

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Online bullying

6.1 Definition

Online 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.)

6.2 Preventing and addressing online bullying

To help prevent online 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 online bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss online bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online 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 online bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school offer's parents access to the safer schools app which gives up to date information on e-safety and which games/apps are unsafe.

In relation to a specific incident of online 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.

6.3 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 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

7. Acceptable use of the internet in school

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. 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school these must be handed to the teacher and locked away until the end of the day. They are not permitted to use them during the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the Acceptable use policy.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices should not contain personal data relating to the school must be encrypted if they do. Staff are encouraged to save files needed to work on at home to OneDrive or share point.

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

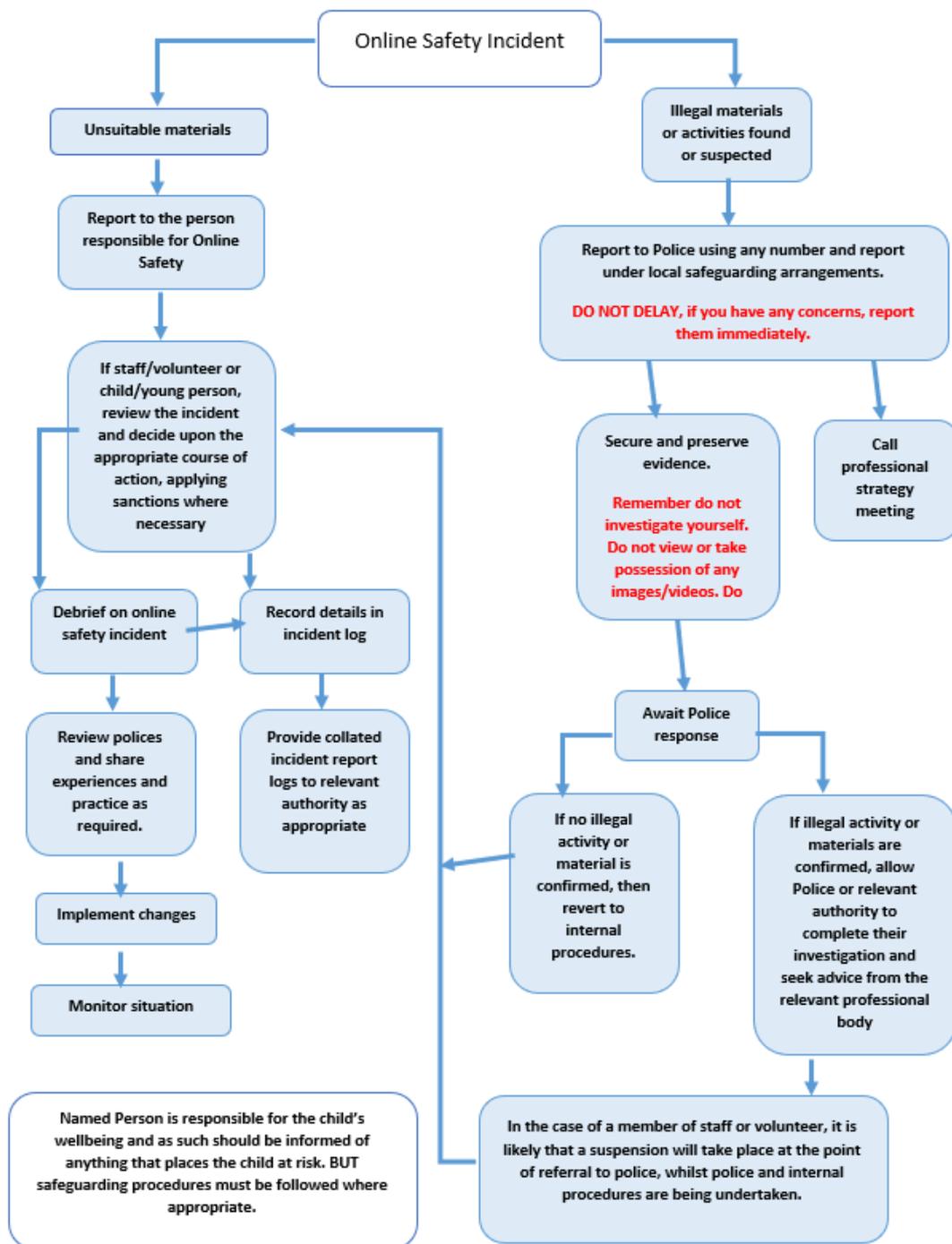
Work devices must be used solely for work activities. Staff should be aware that the devices are still monitored whilst off site.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, 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. 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. Please use the flow chart below to assess the incident:



11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including online 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).

The DSL/DDSL 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log should be made on 'ischools'.

This policy will be reviewed every year by the Computing leader and DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- PREVENT and Radicalisation policy

14 . Online safety policy Covid 19 addendum

Mental health

Negative experiences and distressing life events, such as the current circumstances, can affect the mental health of pupils and their parents. Teachers should be aware of this in setting expectations of pupils' work where they are at home.

There they are providing for children of critical workers and vulnerable children on site, schools should ensure appropriate support is in place for them. Our guidance on mental health and behaviour in schools sets out how mental health issues can bring about changes in a young person's behaviour or emotional state which can be displayed in a range of different ways, and that can be an indication of an underlying problem. Support for pupils and students in the current circumstances can include existing provision in the school (although this may be delivered in different ways, for example over the phone) or from specialist staff or support services. You can read the guidance on [mental health and behaviour in schools](#).

Online safety in schools

- It will be more important than ever that Hillary will provide a safe environment, including online.
- School will continue to ensure that appropriate filters and monitoring systems (read [guidance on what "appropriate" looks like](#)) are in place to protect

children who remain in school when they are online on the school's IT systems or recommended resources.

- LA ICT will maintain safe IT arrangements. LA ICT has a team on hand so if anyone because unavailable there is always someone to support school.

The [UK Council for Internet Safety provides information to help governing boards and proprietors assure themselves](#) that any new arrangements continue to effectively safeguard children online.

The [UK Safer Internet Centre's professional online safety helpline](#) also provides support for the children's workforce with any online safety issues they face. Local authorities may also be able to provide support.

Children and online safety away from school.

School should be doing what they reasonably can to keep all of their children safe. In most cases, the majority of children will not be physically attending the school.

It is important that all staff who interact with children, including online or by telephone, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the child protection policy and where appropriate referrals should still be made to children's social care and as required the police. Staff should continue to follow school safeguarding protocol via ischool and report concerns to the safeguarding team. School should consider the safety of their children when they are asked to work online from home;

- The starting point for online teaching should be that the same principles as set out in the school's staff behaviour policy (sometimes known as a code of conduct).
- This policy should amongst other things include acceptable use of technologies, staff pupil/student relationships and communication including the use of social media. The policy should apply equally to any existing or new online and distance learning arrangements which are introduced.
- Communication with children and parents can only be via professional online platforms such as work emails, purple mash and class charts. There should be not contact with parents via personal social media accounts.
- School can communicate with parents and children via official social media accounts owned by school. Only allocated staff can update these accounts.
- Any phone calls made home to parents via personal devices must have withheld numbers and only if teachers feel comfortable in doing so.
- Children who are being asked to work online have very clear reporting routes in place via our school website so they can raise any concerns whilst online. As well as reporting routes back to the school. The website and school social media accounts will signpost children to age appropriate practical support.

Our school website provides helpful links to parents and children for online support such as:

- [Childline](#) - for support
- [UK Safer Internet Centre](#) - to report and remove harmful online content
- [CEOP](#) - for advice on making a report about online abuse

And many more.

During Covid 19 school will in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school their child is going to be interacting with online. When homework is set via class charts an announcement to parents can be sent.

Parents and carers may choose to supplement the school online offer with support from online companies and in some cases individual tutors. In their communications with parents and carers, school should emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children. Support for parents and carers to keep their children safe online is found on our school website and includes:

- [Internet matters](#) - for support for parents and carers to keep their children safe online
- [London Grid for Learning](#) - for support for parents and carers to keep their children safe online
- [Net-aware](#) - for support for parents and carers from the NSPCC
- [Parent info](#) - for support for parents and carers to keep their children safe online
- [Thinkuknow](#) - for advice from the National Crime Agency to stay safe online
- [UK Safer Internet Centre](#) - advice for parents and carers

Pupil Acceptable Use Policy Agreement - Early Years



✓ I tap or click on things I have been shown.

✓ I ask before I use a tablet, computer or camera.

✓ I check if I can tap/click on things I haven't seen before.

✓ I tell a grown-up if something upsets me.

My name:

Date:

Pupil Acceptable Use Policy Agreement - Key Stage 1



This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):

Date:

Pupil Acceptable Use Policy – KS2



Agreement

KS2

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.
 - T = Is it true?
 - H = Is it Helpful?
 - I = Is it Inspiring?
 - N = Is it Necessary?
 - K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

My name:

Date:

Acceptable use policy for staff

Introduction

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection regulation together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information. If you are in doubt and require clarification on any part of this document, please speak to the Head Teacher/Online safety lead.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the Head Teacher/Online safety lead. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage. The Head Teacher/School Business Manager are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

Network access and security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the SLT for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Head Teacher/Online safety lead as soon as possible.

Users should only access areas of the schools computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Head Teacher/Online safety lead.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

Digital photography

The school encourages the use of digital photography and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press will not include pupil names.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones.
- All photos should be downloaded to the school network
- The use of personal mobile phones for taking photos of pupils is not permitted, a school phone is provided for this purpose. Photos are immediately downloaded and then deleted from the phone

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The school provides a trip ipad for this purpose.
- All phone contact with parents regarding school issues will be through the school's phones. Personal mobile numbers should not be given to parents at the school.
- During Covid 19 personal phones can be used as long as the staff member is happy to do so. However, they must remove caller ID.

Social networking

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via the officially recognised school site and with the permission of the Head Teacher or the Deputy Head Teacher.
- Members of staff will notify the Head Teacher/Online safety lead if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (online bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by Walsall Council Monitoring service. SLT and the Online safety lead to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Head Teacher/Online safety lead considers may

amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school user of the network resources/ equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Head Teacher.

I agree to report any misuse of the network to the Head Teacher. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Head Teacher. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Head Teacher.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed Date

Print name