Alumwell
JUNIOR SCHOOL

Online Safety Policy

2025-26

Policy Review

This document will be reviewed in full by the Governing Body on an annual basis.

This document was formally approved by the Governing Body on 10th December 2025.

Date of Review: December 2026

This page left intentionally blank

Table of Contents

This page left intentionally blank

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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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

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

3. Roles and responsibilities

3.1 The governing body

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

The governor who oversees online safety is Mrs A Hill.

All governors will:

- Ensure that they have read and understand this policy
- Ensure they have had training on a regular basis about online safety

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, keeping up to date with current legislation and that this policy is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

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

The Designated Safeguarding leads for school are Mrs L Upton and Mrs L Timmins

Deputy DSL's in school are Mrs K Boam, Ms C Holmes and Mrs L Guy

The DSL/ Deputy 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 headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body
- Ensuring filtering and monitoring is in place on school owned devices and regularly testing this

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager 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 and on school devices, 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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,staff code of conduct and teaching standards, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of online safety incidents 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
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

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.

4. Educating pupils about online safety

Online safety is now a statutory part of the programme of study for all pupils. Rules and technical solutions are not infallible and we are aware that outside school, children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks.

Pupils are taught about online safety in every year group, using a planned progressive online safety curriculum, based on the Dfe guidance document published in June 2020 'Education for a Connected World.' It is provided as part of Computing (through Purple Mash) / RSE (through PHSE lessons) and is regularly revisited throughout the year.

Covering the key strands of:

- Online Relationships
- Online Bullying
- Self-Image and Identity
- Online Reputation
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership.

Additionally, all schools have to teach the following elements alongside the current guidance:

Relationships education and health and education in primary schools

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.
- 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 internet will also be covered in other subjects where relevant. Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Teachers and staff use Twitter to model the safe use of social media, this may take place on a school or personal device, please refer to the school social media policy.

Where pupils undertake searching of the internet, staff encourage children to use child-friendly search engines e.g Swiggle and monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches, this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

The school will use assemblies and events, such as 'Safer Internet Day', to raise pupils' awareness of dangers that can be encountered online and may also invite trained speakers to talk to pupils about this; where appropriate as a way of enhancing the embedded online safety curriculum.

4.2 Rules for keeping safe

Underpinning the ICT curriculum are the SMART rules, which are reinforced in school across the curriculum:

- **Safe** – encourages young people to be safe by not giving out their personal details online.
- **Meeting** – draws attention to the risks associated with meeting someone you only know online.
- **Accept** – highlights the risks of accepting emails, pictures and text messages from unknown sources.
- **Reliable** – is a reminder that not all information found online is necessarily reliable.
- **Tell** – encourages children to tell someone if something happens or they meet someone online that makes them feel uncomfortable, or if they or someone they know is being bullied online.

These rules are reinforced through the following:

- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety with information via our website. This policy will also be shared with parents.

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.

Parents are responsible for pupils behaviour online at home, school may support parents if an incident involves other pupils at school.

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

6. Dealing with online safety incidents

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues are reported to the DSL via CPOMS. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the Headteacher or to the Chair of Governors, if the headteacher is absent or the accusation involves the headteacher this should go to the LADO via Walsall MASH 0300 555 2866.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend.

We encourage children to take responsibility for protecting each other.

6.1 Managing incidents

In the event of suspicion of an infringement of policy on school device then all the following steps should happen:

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images including youth produced imagery, nudes and semi nudes, as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

7. Acceptable use of the internet in school

All pupils, parents, staff and volunteers 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, when using school devices.

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 on school devices visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

8. Technical Issues

Walsall Council Schools ICT support provides technical guidance for Online safety issues for all Walsall schools. The school IT provider provide support for technical issues in school on a daily basis and coordinate with Walsall Council. Technical support visits the school once every three weeks.

Responsibilities – Antivirus, network security, back up's, updates, filtering and monitoring installation

9. Filtering and monitoring

The Walsall Council school internet service is provided by Net sweeper and monitoring is carried out using Smoothwall Monitor via the Walsall Council Online monitoring service. Internet access is filtered for all users by Walsall Council. Illegal content (child sexual abuse images) is filtered by actively employing the Walsall Council. Content lists are regularly updated and internet use is logged and regularly monitored. However, we are aware that no filtering and monitoring is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence, teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that "over blocking" does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools. The school reports issues through logging a call to the service desk. Any filtering requests for change and issues are also reported immediately to the technical team. Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher.

The school implements a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. This is being implemented by Walsall Council Online Monitoring service by:

- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Walsall Council to support the school by drawing attention to concerning behaviours, communications or access
- ability to produce reports on the websites visited by all young people and adults using our systems
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up
- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail

Networked devices and chromebooks are monitored using this system however iPads currently are not. When using iPads in school the internet is filtered, pupils are taught about making the correct choices when online and staff should fully and actively supervise pupils during activities

10. Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

11. Pupils using mobile devices in school

Pupils are only permitted to bring a mobile phone to school if they travel to and from school independently (e.g., walking home alone).

All pupil mobile phones must be:

- Handed in to the school office upon arrival at school.
- Collected from the school office at the end of the school day.
- Not used at any time on school premises.

Please note that phones are brought into school at the parent's own risk. While we will do our best to store them securely, the school cannot accept responsibility for any loss, damage, or theft.
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 confiscation of their device.

12. Parents and carers using mobile phones

Parents, carers, and visitors are not permitted to use mobile phones anywhere on school premises, including playgrounds, corridors, and classrooms, to protect the privacy and safety of all pupils.

13. Staff devices

13.1 Staff using work devices outside of 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)
- Making sure the device locks if left inactive for a period of time
- The device can be used for personal use but staff are reminded that this monitored so all staff should be mindful of all activity taking place on it
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

- Staff members must not use the device in any way which would violate the school's terms of acceptable use
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager

12.1 Staff mobile devices in school

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. Mobile phones may be used in staff room or

offices where children are not present, but this use should be minimised. The desired option is for phone calls to be made outside of the school building or in the staff room or designated offices. The only exception to this is in case of emergency during a school trip. Staff may wear Smart watches/technology but these should be silenced during teaching time and staff should not respond to alerts/notifications.

If Staff use their own mobile phone to take images of children, for example on a school trip, staff should download and delete these images immediately. These should not be stored or backed up in anyway, backups should be deleted straight away too.

14. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

15. Social media policy – access from personal devices

14. Internet and Network access

14.1 Visitors to school including Governors

Visitors and governors can gain access to Wi-Fi on personal devices. The Wi-Fi is password protected and they will need to ask for the password first. All internet activity is filtered. Any guest/visitor users are given the student internet access where internet is heavily filtered.

14.2 Staff access

Staff can access the school Internet via a school devices and can access the school Wi-Fi on personal devices but should be mindful of what they are doing on devices.

14.3 Communications Technologies

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.

Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.

Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site (Governor Hub) that governors can access to via a personal user account.

Personal email addresses, text messaging, public chat and social networking programmes are not being used for communications with parents/carers and children.

Personal information is also not posted on the school website.

14.4 Personal Social Media use

Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.

Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community

Personal opinions are not attributed to the school

Security settings on personal social media profiles are regularly checked to minimise risk

Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.

15. Use of Digital Images and Videos

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of

misuse and has the potential to be used for online bullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, or newsletter. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the General Data Protection Regulation. However, in order to protect other children and respect privacy these images should not be published or made publicly available

on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

- Pupils' work is only published with the permission of pupils and parents / carers.

16. Training

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

17. Monitoring arrangements

All staff are responsible for logs of behaviour and safeguarding issues related to online safety on CPOMS. An incident report log will be sent to school from the Walsall Online monitoring service and this will be downloaded by Mrs K Boam or Mr T Barton to be dealt with and logged on CPOMS.

18. Online Safety and Emerging Technologies

As part of our commitment to safeguarding pupils in a rapidly evolving digital landscape, the school recognises the importance of addressing risks associated with emerging technologies. These include, but are not limited to:

- Artificial Intelligence (AI) and Chatbots
- Augmented and Virtual Reality (AR/VR)
- Deepfakes and Synthetic Media
- Online Scams and Phishing
- Smart Devices and Internet of Things (IoT)
- Online Gaming and In-game Communication
- Curriculum Integration

Pupils will be taught to critically evaluate content generated by AI tools and understand the risks of misinformation and manipulation.

Lessons will include awareness of deepfakes and synthetic media, helping pupils recognise altered content and understand its implications.

Online gaming safety will be addressed, including risks of grooming, in-game purchases, and exposure to inappropriate content.

- Staff Training

Staff will receive annual updates on emerging technologies and associated risks.

- Training will include how to support pupils in navigating new platforms safely and how to respond to incidents involving emerging tech.

- Technical Safeguards

- The school will work with its IT provider and Walsall Council to ensure filtering and monitoring systems are updated to detect and respond to threats from emerging technologies.
- Any new devices or platforms introduced into the school will be risk-assessed for online safety implications.

- Pupil Support

- Vulnerable pupils will receive additional guidance and support in understanding and managing risks related to emerging technologies.
- Pupils will be encouraged to report any concerns related to new technologies, including suspicious messages, scams, or inappropriate content.

- Parental Engagement

- Parents will be informed about emerging technologies through newsletters, workshops, and the school website.
- Guidance will be provided on how to support children in using new technologies safely at home.

19. Links with other policies

This Online Safety Policy is linked to our:

- Child protection and safeguarding policy
- Relationships and Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1 - Provision of ICT Systems

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

Users must not try to install any software on the ICT systems without permission from the Headteacher/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 Headteacher/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 (this means they should have a mix of capital letters, numbers and punctuation). They should not be the same as any other passwords. Staff should be using a password manager. 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 Headteacher/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. The computer systems auto lock unless presenter mode is used when staff need to remember to lock their computer. 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.

When using our email/communication systems to communicate with parents, all emails will be saved. Communication with our families will be professional in tone and manner.

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 Headteacher/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 Images

The school encourages the use of digital cameras 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
- Personal mobile phones/devices can be used for taking images of pupils, images are immediately downloaded and then deleted from the phone/device

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.
- All phone contact with parents regarding school issues will be through the schools phones. Personal mobile numbers should not be given to parents at the school.

Social networking

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 Headteacher or the Deputy Headteacher.
- Members of staff will notify the Headteacher/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 (cyber 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 Smoothwall. 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 the Headteacher/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.