Weaverthorpe C.E. Primary School

E-Safety & Social Media Policy (including Acceptable Use Agreements)

Adopted by: IEB
Spring2 2021

Review date: Spring2 2024

Contents

Scope

This policy applies to:

- all electronic devices including computers, phones and other SMART devices such as televisions, toys and gadgets
- all capabilities of such devices including running applications, internet connection, recording and displaying voice and image (still and video), communication (including voice, messaging, visual (e.g. Microsoft Teams, Skype, Zoom), games and other applications)
- the use and contents of such devices by staff, pupils, governors and visitors to school including parents, advisors and contractors whilst on school premises or engaged in school related activities, e.g. trips and sports meetings
- external provision of services including web server, website, software & hardware
- all digital data including any transferred to other media including printouts, screen prints and written notes

Objectives

The policy aims to protect all those associated with the school from harm through the use of electronic devices by:

- providing a clear definition of what is considered harmful
- providing education and guidance to staff, pupils, governors and parents regarding:
    - not using devices for harmful purposes
    - how to prevent exposure to harmful uses
- monitoring and preventing, as far as possible, the use of school devices for harmful purposes
- clarifying the school's right to monitor the use and content of personal devices
- identifying responsibilities of all parties in providing and achieving safety.
- meeting Ofsted expectations

Policy Maintenance

This policy is based on guidance provided by NYCC
https://cyps.northyorks.gov.uk/sites/default/files/Safeguarding/Online%20Safety/Final%20September%202020%20Online%20Safety%20Guidance%20for%20Schools%20and%20Settings%20in%20North%20Yorkshire.pdf
which can be viewed for further detailed advice and guidance on information and training resources.

The Governing Board will review the policy annually.

The responsible Governor and named member of the Senior Leadership Team will review the policy termly to ensure:

- responsibilities are being met
- it addresses developments in technology and its use
- it addresses any E-Safety incidents recorded in the School's incident log

and, if necessary, propose immediate amendments to the Governing Board.

Responsible Governor – Carolyn Childs (SEN and Safeguarding)

Named Member of the Senior Leadership Team – Rachel Ray (Head Teacher)

A copy of this policy will be available on the school website.

Related Policies

This policy addresses a specific issue more broadly covered in other policies, e.g.:

- Child Protection
- Risk management
- Anti-Bullying
- Behaviour
- Relationships and Sex Education
- Data Protection

Roles & Responsibilities

Note that the NSPCC provides comprehensive guidance on e-safety which is a useful resource – see https://www.nspcc.org.uk/keeping-children-safe/online-safety , also https://www.net-aware.org.uk

Governing Board

In reviewing this policy, the Governing Board will ensure: -

- that the policy is disseminated to all relevant and interested parties
- that agreed actions have been undertaken
- that policy objectives are being achieved
- that the statutory requirements of Keeping Children Safe in Education (Sept 2020) are complied with. Specifically, in relation to online safety, ensuring that: -
    - staff undergo relevant training,
    - pupils are taught about safeguarding, including on-line, as part of a broad and balanced curriculum
    - pupils are safeguarded from potentially harmful and inappropriate online material by appropriate monitoring and security systems
- regular monitoring and appropriate responses to e-safety incidents
- complete e-safety training
- use their governor and not personal login to access information and communicate on school matters
- that the responsible Governor has the necessary up to date training to identify and address e-safety risks and is familiar with the guidance from NYCC.

Headteacher

The Headteacher is responsible for providing an e-safe environment including:

- communicating to all relevant parties:
    - advice on e-safety and awareness
    - the school's e-safety provisions, requirements and sanctions.
    - procedures for reporting suspected or actual e-safety breaches
    - the school's policy on monitoring individual activities and personal devices
- monitoring e-safety related risks and violations
- reporting and addressing identified risks, suspicions and actual violations of e-safety
- updating the policy, procedures and training in the light of experience and new developments, e.g. in technology

- staff will receive training on:
    - identifying possible breaches and risks
    - identifying child protection issues relating to e-safety
    - personal responsibilities for use of technology, e.g. use of personal phones and social media
- advising parents on e-safety outside the school environment and support in talking to children about these issues
  NB: Whilst the school can have limited powers in relation to out of school activities by pupils and none for parents, making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly, threats of violence can lead to criminal proceedings under the Malicious Communications Act.
- liaising with external parties including visitors, contractors and service providers to ensure that:
    - they are aware of the school's no tolerance policy towards any activity, public or personal, violating the school's e-safety
    - all contracts providing technology services to the school include adequate provisions, as appropriate, for effective filtering, monitoring and security
    - the security provided for the school's website denies inappropriate access and the company hosting it has an action plan and key contact if it is 'hacked'
    - advice is obtained as needed to verify the technical content of contracts and agreements
- Ensuring e-safety is embedded in the curriculum and forms part of the RSE teaching
- Maintaining and regularly reviewing a record of e-safety incidents

All Staff

All staff will: -

- sign the school Staff Acceptable Use Agreement (see Appendix2) to confirm that they have read, understood, and agree to comply with it.
- receive training in e-safety and broader risk and child protection topics
- are responsible for raising any concerns or additional requirements they identify
- ensure pupils understand and follow the school's on-line safety and acceptable use agreement
- use opportunities within the curriculum & other school activities to embed e-safety
- monitor pupils for signs of e-safety violations and distress caused by e-activity
- in lessons where Internet use is pre-planned, guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

Staff are expected to be professional in their use of technology, in particular they should: -

- not 'befriend' any pupil or pupil family member on social media in a social context whilst the pupil is at the school
- be aware that emails can be part of Freedom of Information requests and all correspondence needs to be professional, courteous and respectful
- ensure that all confidential information / information under the Data Protection Act must only be transmitted through a secure system

ICT Technical Service provider

The ICT technical service provider is responsible for ensuring that: -

- the school's ICT infrastructure is secure and meets requirements for filtering and monitoring
- the school's password policy is adhered to
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- the use of the school's ICT infrastructure (network, remote access, email, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the named SLT for action.

For this purpose they are expected to be up to date with online safety technical information.

Designated ICT technical service provider: NYCC

Pupils

All pupils: -

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement (see Appendix 2), which they will be required to sign before being given access to school systems
- should understand the importance of reporting abuse, misuse or access to inappropriate materials to a member of staff
- will not use any technology or SMART device in school or during school activities without the express permission of a member of staff which can be refused if safety cannot be assured
- will not use technology or SMART devices to abuse, disrespect or reveal personal information or images relating to the other pupils or anyone associated with the school.

Parents and Carers

While the school will teach e-safety and enforce it during school hours and activities, parents and carers are responsible for the appropriate use of technology in other circumstances. They should also be aware of the health effects of screen time and social media on children. Screen time should be balanced with physical/other activities and sleep. A number of systems and apps are available that can limit the screen time for children and young people, alongside parents and carers talking to their children about the issues

Parents and carers are responsible for: -

- signing the Parents Acceptable Use Agreement (see Appendix 2) and countersigning the Pupil Acceptable Use Agreement for those in their care.
- signing a photo/video release slip when their child starts school; non-return of the permission slip will not be assumed as acceptance.
- accessing the school website and corresponding with the school in accordance with the Parents Acceptable Use Agreement
- ensuring that they do not use social media to criticize or make inappropriate comments about the school or an individual member of staff, as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly, threats of violence can lead to criminal proceedings under the Malicious Communications Act.

- contacting the school directly if they have any concerns about e-safety

Monitoring the use and contents of technology

The school recognises that everyone has a right to privacy but must balance this with its obligations for security and safeguarding.

Monitoring may therefore be undertaken to:

- identify potential and actual inappropriate or illegal activity (deliberate or accidental)
- obtain evidence to support disciplinary action if necessary.

Where active monitoring is in place, reasonable efforts will be made to inform users in accordance with the Data Protection Act.

Staff may also undertake spontaneous monitoring when there is reasonable suspicion of inappropriate or illegal activity. The reason will be explained to those involved but consent is not required and refusal to comply will itself be considered actionable.

Appendix1 - School Technology

Assistive Technology

Weaverthorpe School uses a range of devices including PC's, laptops and tablets. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use virus protection software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Headteacher and IT Support[1] are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use software that prevents any infected email being sent from the school or received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No personal pupil data that is not linked to teaching and learning, is to leave the school in an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – *A*ll staff, pupils and governors will be unable to access any device without a unique username and password. Staff and pupil passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated automatically for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the Staff Acceptable Use Agreement and pupils upon signing and returning their acceptance of the Acceptable Use Policy. Parents should also sign this agreement

Email – All staff and governors are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Pupils are not permitted to use the school email system.

[1] IT Support is provided by NYCC

Photos and videos – Digital media such as photos and videos are covered in the schools' Child Protection Policy. All parents must sign a photo/video release slip when their child starts school; non-return of the permission slip will not be assumed as acceptance.

Social Networking – Weaverthorpe School recognises the use of social networking as a tool to engage with parents and the wider school community. The following social media services are permitted for use within Weaverthorpe School and have been appropriately risk assessed. Should staff wish to use other social media; permission must first be sought via the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and pupils in school via the school website.
- Twitter – used by the school as a broadcast service

A broadcast service is a one-way communication method in order to share school information with the wider school community.
In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the Headteacher who will assist you in taking the appropriate action to deal with the incident and filling out an incident log (see Risk Management Policy)

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Weaverthorpe School will provide training as necessary which is suitable to the audience.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning.

Should any member of staff feel they have had inadequate or insufficient training generally or in any area this must be brought to the attention of the Headteacher for further CPD.

Appendix 2 – Acceptable Use Agreements

Acceptable Use Agreement – Staff

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.
Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.
The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below.
Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.

- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the headteacher in writing for each occurrence.
- •I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person.
- Any school trips/outings or activities that require a mobile phone/camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point- will I use my own devices for capturing images/video or making contact with parents/carers

Staff Name:

Signature: Date:

Acceptable Use 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.

I understand this agreement and know the consequences if I don't follow it.

Name: Class:

Parent/Carer Signature: Date:

Acceptable Use Agreement – KS1

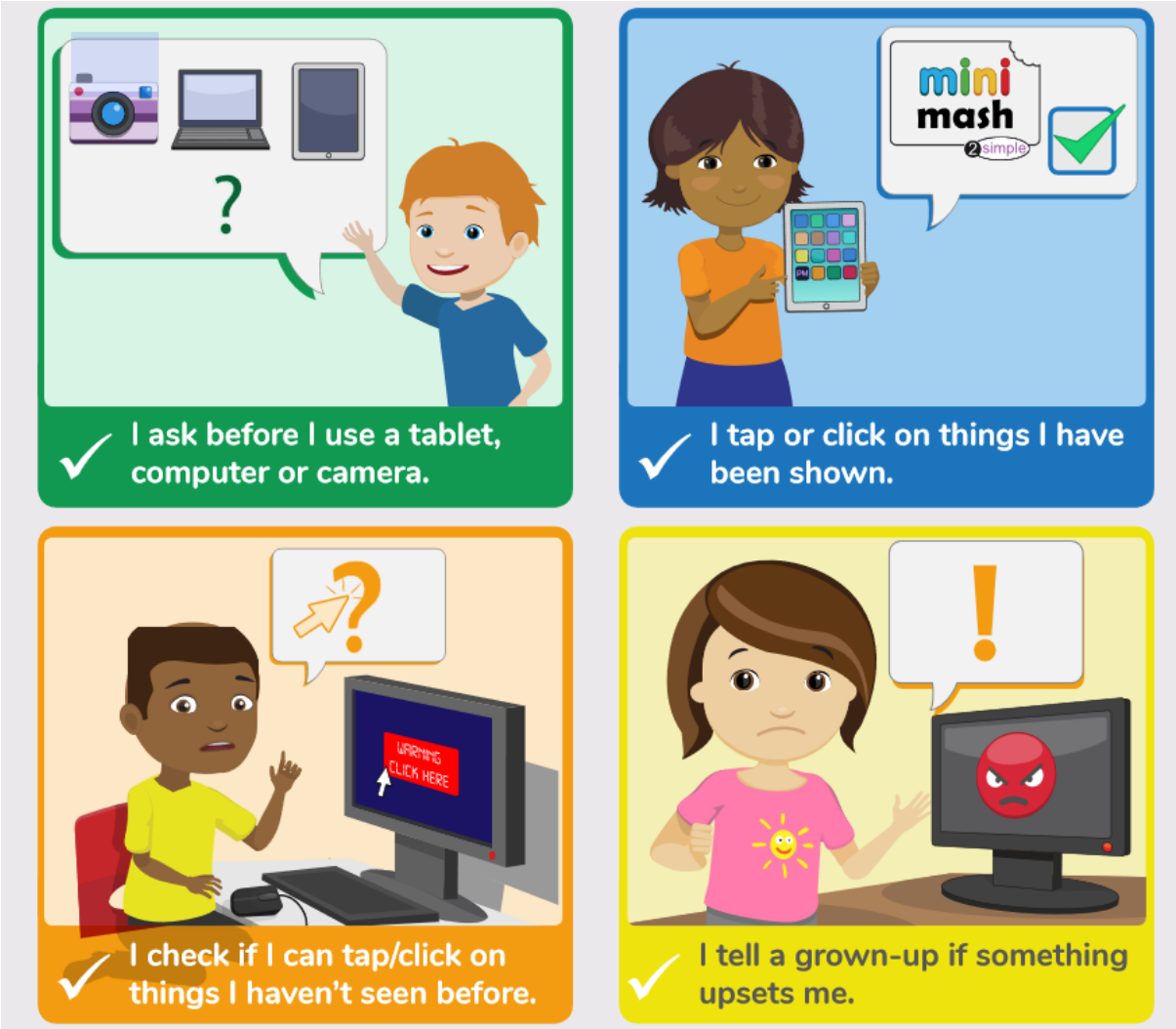
- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online
.
- I know I must never communicate with strangers online.
- I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

Name: Class:

Parent/Carer Signature: Date:

EYFS Acceptable Use Agreement



Name: Class:

Parent/Carer Signature: Date:

Acceptable Use Agreement – Parents/Carers

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This **Parent/Carer Acceptable Use Agreement** is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Parents/Carers

We ask parents and carers to support us by:

- Sharing good online behaviours with your child.
- Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- Explaining how to keep an appropriate digital footprint.
- Discussing what is and isn't appropriate to share online.
- Emphasising never to meet anyone online nor trust that everyone has good intentions.
- Reporting any concerns you have whether home or school based.
- Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Permission Access

By signing below, you agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Your Child's Name: Class:

Parent/Carer's Signature: Date:

*The school aims to comply with GDPR regulations at all times and as such follows strict protocol about how we use personal data and keep it safe, including the information on this form. It is important that you refer to the school's data protection policy or contact the school if you have any questions about data.

Appendix 3 – Additional Guidance on Safe and Acceptable Use.

Unacceptable Content

In using email and the internet Users must understand that:

- Usage must not tarnish the reputation of the School,
- No communication should be sent that can be interpreted as insulting, disruptive, or offensive by any other individual or entity including:
    - Sexually explicit messages, images, cartoons, jokes or movie files,
    - Unwelcome propositions,
    - Profanity, obscenity, slander, or libel,
    - Ethnic, religious, or racial slurs,
    - Political beliefs or commentary,
    - Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- they should not use the internet in a way which could affect usage for others including not streaming or downloading media files and not using the internet for playing online games.
- School management may have access to their internet browsers and browsing history, which should not be deleted, and reserves the right to suspend internet access at any time.

Use for Non-school Business

School ICT resources, including email and internet, should not be used for any personal or other business including work for political organisations, not-for-profit organisations, and private enterprises.

Email Security

Users will take care to use their email accounts in accordance with the School's information security policy. In particular, users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the School's IT network,
- Not send excessively large email attachments without authorisation from School management and the School's IT provider.

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights.