ST MARY'S

Church of England Primary School

I.C.T & Internet Acceptable Use Policy

2024 - 2027

St Mary's C of E Primary

Name of Policy: I.C.T & Internet Acceptable Use Policy

Author: Carol Benson

Adopted following governor approval: December 2023

Updated: December 2024

Review date: December 2025

This school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment. Please report any safeguarding or child protection concerns to the designated teachers for Child Protection:

Mrs Benson, Mr Butterwick & Miss Clayton

The Governors and Staff of St Mary's CE Primary School are committed to educating the children spiritually, academically, emotionally and physically within a distinctive Christian ethos.

"Together we nurture and inspire so that everyone can flourish"

"What shall we say the kingdom of God is like, or what parable shall we use to describe it? It is like a mustard seed, which is the smallest of all seeds on earth. Yet when planted, it grows and becomes the largest of all garden plants, with such big branches that the birds can perch in its shade."
The parable of the mustard seed. Mark 4:30-32

Love, respect and moral understanding lie at the heart of the ethos of St Mary's Church of England Primary School. We see our learners as the future custodians of God's world. We aim to nurture and encourage happy individuals who are socially engaged and curious about life within and beyond their own community. We value and encourage difference and diversity. St Mary's is a nurturing, safe place for children to question, to learn to love and respect other people and to discover their place in the world. We have traditional values, rooted in the Christian faith, as well as global, 21st Century aspirations for all our pupils.

St Mary's is part of the Wharfe Valley Learning Partnership, a collaborative of schools in Wetherby and Boston Spa, where the vision for all children is to be respectful, globally aware and compassionate as well as ambitious, resilient and engaged in their learning.

Introduction

ICT is an integral part of the way our school operates. It is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Due to the ramifications of non-compliance, breaches of this policy may be dealt with under our Behaviour Policy or Staff Discipline Procedures.

Aims of this policy:

- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school in teaching pupils safe and effective internet and ICT use.
- To promote the safety of learners in our care both in school and elsewhere.

St Mary's C of E Primary School Responsibilities:

- To provide the correct ICT equipment such as desktops and laptop computers to teaching and support staff.
- To pride pupils with the correct ICT equipment and ensure it has the appropriate access, restrictions and firewalls in place.
- To ensure the smooth running of all ICT equipment.
- To ensure the correct firewalls and internet safety software is in place and operating correctly.

School Staff Responsibilities:

- To ensure correct use of ICT equipment at their disposal.
- To look after and respect the ICT equipment in school.
- To ensure ICT equipment is returned to the correct location after each use and is placed on charge so it is ready to the next user.
- To support the educate children and the wider community in the acceptable use of ICT equipment.
- To ensure proper compliance with this policy

Office Staff:

- To ensure correct use of ICT equipment at their disposal.
- To look after and respect the ICT equipment in school.
- To ensure ICT equipment is returned to the correct location after each use and is placed on charge so it is ready to the next user.
- To support the education of children and the wider community in the acceptable use of ICT equipment.
- To ensure proper compliance with this policy

Head Teacher:

The head teacher will be responsible for ensuring all staff understand and comply with is policy as well as to monitor the ICT equipment and contracts pertaining to the ICT equipment.

Governors :

Governors will ensure that staff have signed for an understand the information provided in this policy document.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools

Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose.
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities. This includes the head teacher and designated e-safety leader and may include other staff depending on the nature of the system/facility.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.
- **"Filtering & Monitoring":** all employees, lead and informed by the appointed DSL, as part of schools Prevent Duty should filer and monitor websites accessed by children to ensure appropriate and safe content is accessed.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary proceedings (see sanctions).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without consent (see 'internet access' below as well as refer to schools BYOD Policy)
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of

software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher and Computing Subject Leader/Internet Safety Officer will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteachers discretion. Examples could include:

1. Fact-finding in order to assist a child who has become the victim of cyberbullying ('accessing offensive material').
2. Deliberate testing of the school's digital safeguarding facilities by relevant staff or the Education and Early Years Safeguarding Team.

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's Behaviour Policy or Staff Disciplinary Procedures.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's curriculum network is managed by Vital Ltd. (York). The school's administrative network is managed by Schools ICT (Leeds). This management of the school's ICT facilities and materials includes, but is not limited to:

1. Computers, tablets and other devices
2. Access permissions for certain programs or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. They will be required to re-set their password periodically.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Computing Subject Leader/Internet Safety Officer, school office or Head Teacher.

Use of phones and email

The school provides each member of staff with an email address. This email account should be used for work purposes only.

Should a staff member realise that they have inadvertently used their work email for personal communication they should discuss this with the Head Teacher or the designated e-safety leader at the first opportunity.

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

All work-related business should be conducted using the email address the school has provided.

Bulk message for whole class or whole school communication should be sent by the school office or Head Teacher using the schools MIS system so a permanent record of the communication can be retained.

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

If a staff member is worried they have received an email that uses incorrect or improper statements they should discuss this with the head teacher or the designated e-safety leader at the first opportunity.

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

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. There may be times when a staff member is required to use the Leeds City Council-approved Mail Express system. Advice on this can be obtained from Designated Safeguarding Leads (DSLs) in school.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the data protection officer or the head teacher immediately and follow our data breach procedure which forms part of our Data Protection Policy.

Staff must not give their personal phone numbers to parents, carers or pupils.

Staff must not use their personal phones to contact parents or pupils, there are three phones located in school which can be used to phone parents, carers or pupils.

In certain circumstances, with the authorisation of the head teacher, staff may wish to use their personal phone number as a contact for other staff and other adults with a supervisory role (for example, when leading a school trip). Staff should remember that only volunteers who have been DBS and barred list checked by the school should have a supervisory role in such a circumstance. It is therefore not advisable for staff to share their phone numbers with volunteers accompanying trips who are not in this role.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher and network manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

1. Does not take place during contracted working hours.
2. Does not constitute 'unacceptable use', as defined above.
3. Takes place when no pupils are present.
4. Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff who use the school's ICT devices to store personal non-work-related information or materials (such as music, videos, or photos), should note that school does not take responsibility for the security of this data and they should remember that the device they use remains the property of the school and may be recalled or monitored at any time without notice.

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

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Internet Safety Policy, Bring Your Own Device Policy, and this document. They must not be used during contracted working hours, unless in the case of an emergency.

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

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is always appropriate.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

School social media accounts

The school has an official Twitter page, managed by the Computing Subject Leader/Internet Safety Officer. Staff members who have not been authorised to manage, or post to, the account must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to

the extent permitted by law.

The school monitors ICT use in order to:

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

Pupils

Access to ICT facilities

Computers, tablets and mobile devices are available to pupils only under the supervision of staff.

Pupils will be provided with an account linked to the school's Google domain, which they can access from any device – in or out of school - by using their Google credentials, provided by Vital Ltd. (York).

Internet service and filtering are currently provided by EXA Networks (Bradford).

Search and Deletion

Pupils are not permitted to have mobile phones in school. Some parents of children in upper Key Stage 2 may wish for them to have a mobile phone for safety reasons if they walk to and from school on their own. If this is the case, pupils must hand their mobile phone in at the school office or the class teacher upon arrival, then collect it prior to leaving at the end of the school day.

Mobile devices are brought to school at the owners risk.

Where applicable: Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation. Should a device contain material deemed inappropriate and the possession of the device disruptive to teaching/in breach of school rules, the school has the right to confiscate the device pending further investigation and dialogue with parents.

Unacceptable use of ICT and the internet outside of school

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

- Using school ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school community.
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access

to the school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

Please see the "Serious Behaviour" section of the school Behaviour Policy for further details.

Parents

Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

Parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the Friends of St. Mary's) may be granted an appropriate level of access or be permitted to use the school's facilities at the head teacher's discretion. This may include access to the school's Wi-Fi.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to read the guidance in appendix 2.

Data security

The school takes steps to protect the security of its computing resources, data and user accounts, however, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities are initially provided with passwords. Pupils cannot change theirs but are taught about password security in-class. Adults should set strong passwords for their accounts and keep these passwords secure.

All users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. This is particularly relevant with increased use of Google Apps throughout school and the collaborative capabilities of Google Docs, Slides etc.

Adult users will automatically be reminded to change their password periodically.

Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. This is controlled by Vital Ltd. (York).

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. Our Data Protection Policy is available readily available from the school office.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by Vital Ltd. (York).

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Computing Subject Leader/Internet Safety Officer immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. This applies to all stakeholders. Pupils are taught about this in-class. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

In order to access the Leeds Extranet Portal staff must have access to an incognito window on their browser in order to comply with the Leeds data protection procedures. Vital Ltd (York) must give users additional administrator permissions to do this, the head teacher is responsible for who in school can have this access, currently this is only the head teacher and school office.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff should only use school devices to access school data, to work remotely or take data out of school. They should not use USB drives or any other portable device to take data out of school.

All devices taken out of school which contain school data should be password protected.

Internet access

The school Wi-Fi internet connection is secured.

All users connect to the same Wi-Fi network, via access points throughout the site.

Internet filtering is provided by EXA Networks (Bradford).

Internet filters are not entirely foolproof so if inappropriate material is accessed it must be immediately reported to the Computing Subject Leader/Internet Safety Officer, who can ensure that EXA Networks block the site from which the material came.

The Computing Subject Leader/Internet Safety Officer is able to log on to the Exa Portal and block inappropriate sites as soon as they are located. This process takes no more than ten minutes. Staff should ensure they report the website address correctly and in full to ensure the site is correctly blocked.

Pupils

Pupils have access to the internet on all laptops and tablets used in school. These are permanently connected to the Wi-Fi, with access gained once the pupil is logged-on.

Appropriate security and filtering is provided by EXA Networks as the internet service provider (ISP) and Vital Ltd. (York) who set up and maintain all Google accounts.

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific consent is given.

Consent may be given, for example, in these circumstances:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the FOSM)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Visitors needing access to the school's Wi-Fi must be made aware of this policy and schools Bring Your Own Device Policy. Copies of the password will then be available in the school office.
- Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action. If in any doubt, they must consult the head teacher or e-safety leader.

Monitoring and review

The Headteacher and Computing Subject Leader/Internet Safety Officer monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year as a minimum.

The governing board is responsible for approving this policy.

Related School Documents & Policies

This policy should be read alongside the following school documents:

KCSIE Sept 2023
Internet Safety
Social Media
Bring Your Own Device
ICT and Computing
Safeguarding and Child Protection
Behaviour
Staff Disciplinary
Data Protection

Appendix 1: Reference to Social Media Policy

PRINCIPLES

- All users of social media applications should bear in mind that the information they share, even if on private 'spaces', is still subject to copyright, data protection and Freedom of Information legislation, as well as the Safeguarding Vulnerable Groups Act of 2006.
- Social networking applications must not be used by employees for personal use during working hours, unless the express permission of the Head teacher is obtained.
- Any proposed use of social networking applications as part of a school service/activity (whether they are hosted by the school or by a 3rd party) must be approved by the Head teacher first.

School users must adhere to the following Terms of Use:

Social media applications:

- must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages; this includes, but is not limited to, material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- must not be used for the promotion of financial interests, commercial ventures that result from your association with the school or personal campaigns that may affect the reputation of school.
- must not be used in an abusive or hateful manner.
- must not be used for actions that would put the employees, Governors, or children in breach of school codes of conduct or policies.
- must not breach the school's Disciplinary Policy, Equality Policy, Anti-bullying Policy and Confidentiality Policy.
- must not be used to discuss or advise on any matters relating to school issues, colleagues, children or parents.
- must not facilitate online information-sharing 'friendships' with minors.
- must not identify users as a representative of the school e.g. by using full names.
- must not make reference to any employee, child, parent or school activity or event unless prior permission has been obtained from the Head Teacher.
- must not be used to share out-of-work activities, which may cause embarrassment to the employer or detrimentally affects the employer's reputation. This will result in disciplinary action.
- must not be used by children in an attempt to access a school employee or Governor's area or 'space' on a network.

MONITORING OF THIS POLICY

- Any violation of this policy will be considered as potentially gross misconduct under the school's Disciplinary Policy (Staff); under the Code of Conduct (Governors) and under the school's Behaviour and Exclusion Policies (Children).
- All employees, Governors and children are encouraged to report any suspicions of the misuse of social media applications to the Head Teacher or trusted adult. If the Head Teacher receives a disclosure that an adult employed by the school is using social networking in an inappropriate way as detailed previously, this should be recorded in line with the Child Protection Policy and/or Disciplinary Policy.
- Children are strongly encouraged to report to a trusted adult any worries they have about cyberbullying or improper contact. The school has a duty of care to investigate and work with children and families where there are reports of cyberbullying/misuse of social media applications out of school hours.

THE LAW

- Whilst there is no one specific offence of cyberbullying, certain activities can be criminal offences under a range of different laws, including:

  - The Protection from Harassment act 1997
  - The Malicious Communications act 1988
  - S.127 of the Communication act 2003
  - Public Order Act 1986
  - The Defamation Acts of 1952 and 1996

- A school cannot be 'defamed'; only individuals or groups of individuals can bring action for defamation. Staff who are concerned that comments posted about them are defamatory in nature should seek advice from their union or undertake their own legal advice.
- The Head Teacher will seek legal advice from the Internet Safety Officer and Leeds City Council on any matters related to the misuse of social media applications.

Appendix 2: Acceptable use of the internet: guidance for parents and carers

Acceptable use of the internet: guidance for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels:

- Our website
- E-Mail (accessed via the official school website)

Parents/carers may have also set up independent channels to help them stay on top of what's happening in their child's class, through discussion with one another. For example, through WhatsApp.

These unofficial channels are not approved or regulated by the school, and we urge you to communicate directly with the school if you have a query or question you wish to raise.

We do not accept responsibility for the information or content expressed through such unofficial channels.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, parents should:

- Be respectful towards members of staff, and the school, at all times.
- Be respectful of other parents/carers and children.
- **Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure.**
- It is inadvisable to:
- Use private groups, the school's Twitter page, or personal social media to complain about or criticise members of staff**. A more constructive way is always to contact school staff directly and if necessary use the school complaints procedure.**
- Use private groups, the school's Twitter page, or personal social media to complain about, or try to resolve a behaviour issue involving other pupils. **A more constructive way is always to contact school staff directly and if necessary use the school complaints procedure.**

Parents and carers should note that, if school staff become aware that any inappropriate comments about themselves, their colleagues, their pupils, or any other member of the school community are being made through any online communication channel (albeit official or private/independent and unofficial), the school will take whatever appropriate action is advised by the Leeds City Council legal team.

We also ask that parents and carers do not upload or share photos or videos on social media of any child other than their own.

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

Appendix 3: Acceptable use agreement for older pupils

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

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose.
- Use them without a teacher being present, or without a teacher's permission.
- Use them to break school rules.
- Access any inappropriate websites.
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity).
- Use chat rooms.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Share my password with others or log in to the school's network using someone else's details.
- Bully other people.

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

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

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

I understand that I remain a member of school even when I am at home, and my online behaviour needs to meet school's expectations.

Signed (pupil):	**Date:**

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

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

Appendix 4: Acceptable use agreement for younger pupils

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

Name of pupil:

When I use the school's ICT facilities (like computers and tablets) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me.
- Use them to break school rules.
- Go on any inappropriate websites.
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson).
- Use chat rooms.
- Open any attachments in emails, or click any links in emails, without checking with a teacher first.
- Use mean or rude language when talking to other people online or in emails.
- Share my password with others or log in using someone else's name or password.
- Bully other people.

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know straight away if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that I am still a member of school even when I am at home, and my online behaviour needs to be sensible at all times.

Signed (pupil):	**Date:**

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

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

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let a designated safeguarding lead (DSL) and the e-safety leader know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**