West Twyford Primary School

Acceptable Use Policy

Last reviewed on:	Summer 2024
Next review due by:	Summer 2027
Approved by:	Teaching and Learning Committee

Acceptable Use Policy

This policy was written taking into account advice and guidance in the DfE *Keeping Children Safe in Education Part 1* document, September 2023

Contents

Appendices

A1: Acceptable Use Agreement (Governors, Staff, Volunteers, Placements and other external staff)

A2: Acceptable Use Agreement Pupils – parental consent for Nursery to Y2

A3: Acceptable Use Agreement Pupils – pupils Y3-Y6

A4: Acceptable Use Agreement External Staff - One-off or irregular users

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at West Twyford Primary School (WTPS) with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of WTPS community (including staff, students/pupils, volunteers, parents/carers, Governors, visitors, community users) who have access to and are users of school IT systems, both in and out of WTPS.

Roles and responsibilities

Role	Key Responsibilities
Head Teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (GDPR) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Data Protection Officer: Craig Stilwell Judicium Consulting Ltd 72 Cannon Street, London, EC4N 6AE Email: dataservices@judicium.com Telephone: 0203 326 9174	• Providing advice and guidance when required • Creating and maintaining data records • Drafting data policies and procedures • Providing training for employees • Acting as the first point of contact with authorities • Managing Subject Access Requests and those under Freedom of Information Act • Conducting an annual audit of your data processes

Role	Key Responsibilities
Computing Subject Lead /Designated Child Protection Officer	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Safeguarding Governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the E-Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online Safeguarding Governor will include regular review of the online safety procedures with the Safeguarding Committee.
Computing Subject Lead	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician (TurnITOn)	• To report online safety related issues that come to their attention, to the ICT Coordinator or School Business Manager. • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis

Role	Key Responsibilities
	• That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
School Business Manager (SBM)	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact(s) (currently M. Shapland, M. Spring and A. Hooper)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and student placements.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement. The Acceptable Use Agreement is to be signed by staff annually. The Acceptable Use Agreement is signed by new staff, volunteers and placements on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Frequent external individuals/organisations will sign an Acceptable Use Agreement prior to using technology or the Internet within school • Other external individuals/organisations will be advised of the key parts of Acceptable Use Agreement prior to using technology or the Internet within school. • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/community in the following ways:

- Policy to be posted on the school website/ internal network
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements are signed by staff
- Acceptable use arrangements signed by each pupil on entry to the school and stored in child's individual file.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use and possible sanctions.
- ICT Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to ICT Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Child Protection policy, Anti-Bullying policy, PSHE).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- Provides regular updates and online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should know and understand what the school rules are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively through the school's normal reporting procedures.
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff have been provided with a copy of this policy and that it is available at all times for view on the school network along with other school policies.
- Ensures staff are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- All staff or pupil data must be sent by encrypted email or secure data uploads only.

School website

- The Head Teacher, supported by the School Business Manager and the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to use STRONG passwords for access into our network and MIS system. We advise that all passwords should, where the software, computer, or device allows:
    - be at least 6 characters long including both numbers and letters;
    - be changed on a regular basis [and at least every 180 days];
    - [cannot be the same as the previous 10 passwords you have used];
    - not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Students in Years 5 and 6 (and other students in exceptional circumstances) may request permission in writing from the Head Teacher to bring a mobile device into school. Circumstances may include reasons such as a particular need to contact parents/carers on the journey to and from school. Should permission be granted the student is responsible for delivering the mobile device to the school office at the beginning of the day and collecting the device at the end of the day. The school

accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- Other than with written permission, no students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity..
- No images or videos should be taken on mobile devices except where the device is owned and managed by the school and this is for approved purposes (e.g. ipads for assessment, laptop cameras, curriculum cameras etc) Images should only be stored on the school network and kept within guidelines of the data protection policy.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- It is recognised that the use of personal mobile phones is sometimes practical for the efficient running of school trips and outings. On these occasions staff may provide trip volunteers with access to personal phone numbers. It is not intended that the member of staff's personal contact details be made available for other purposes. Should for any reason a member of staff be contacted directly by a parent, carer or student (except in circumstances where the member of staff is known to the person outside of a professional capacity) the member of staff should advise the Head Teacher at the soonest opportunity. Where the member of staff is known to the parent, carer or student in a capacity outside of the school the member of staff should exercise due caution about the appropriateness of any contact. If any there is any doubt the Head Teacher should be contacted at the soonest opportunity and the details of the conversation discussed.

- On school trips any parent volunteers should be briefed that they may only use mobile phone cameras to photograph their own children.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the GDPR requirements.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Related Policies:

- Data Breach Policy
- Data Protection Policy

Appendix A1

Acceptable Use Agreement:

Our professional responsibilities when using any form of ICT, in or out of school, for our own protection, and for the safety of pupils.

- ☑ ONLY use personal mobile phones in the staff room, office areas or in the classroom and only when no children are present. Agree that mobile phones must not be used in public areas during normal school hours.
- ☑ DO NOT talk about your professional role in any capacity when using social media such as Facebook, Twitter and YouTube. If you wouldn't say it to the headteacher's face, don't put it online.
- ☑ DO NOT put online any text, image, sound or video that could upset or offend any member of the whole school community, or be incompatible with your professional role. If you wouldn't say it in the staffroom, don't say it online.
- ☑ ENSURE all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- ☑ ONLY use school ICT systems and resources (including email & phone) for all school business or in line with what is allowed within the school's procedures.
- ☑ ONLY take photos / videos of pupils and / or staff for professional purposes, in accordance with school's procedures and only using school equipment.
- ☑ NEVER give out your own personal details, (such as mobile, email address or social network profile), to pupils, parents, carers.
- ☑ NEVER disclose any passwords.
- ☑ ENSURE that personal data (such as data held on MIS software) is kept secure and used appropriately. Pupil data or staff files must not be taken off-site except in special circumstances authorised by the Headteacher.
- ☑ DO NOT browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory using school equipment or in school time.
- ☑ BE AWARE that your online activity, both in school and outside school could bring the school into disrepute.
- ☑ ENSURE you know & follow the procedures for reporting any e-Safety incident which may impact on you, your professionalism or the school.
- ☑ READ, understand and adhere to the Acceptable Use Policy.

Signature …….…… Date ……

Full Name ……..Job Title / Role .....

Appendix A2 (appearing as part of the school's registration form)

PARENT/CARER AGREEMENT

As the parent or legal guardian, I give my permission for my child to use the Internet as described in the School's Internet Agreement expectations of pupils using the internet and for as long as they are at the school.

I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and accept responsibility for explaining to my child the school when using the Internet.

Parent/ Carer Signature …….…… Date……

Child's Name..... Class …….

Appendix A3 (appearing as part of the school's registration form)

Primary Pupil E-Safety Internet Agreement

Before your child is allowed to use the internet, we expect all parents/carers and pupils to read and sign this agreement.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not tell other people my passwords OR use any one else's.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- ✓ I will not give private details (home address, mobile number, email address etc) to people I meet online.
- ✓ I will not upload any photos or videos of children in my school on the Internet.
- ✓ I will not arrange to meet anyone I meet online. If someone suggests this, I will tell my parents immediately.

As a school user of the internet, I agree to comply with the above expectations.

Pupil Signature ……Class …… Date……

Appendix A4

External Staff
Acceptable Use Agreement

The school ESafety Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role.

By using your personal mobile device, the school Wi-Fi or ICT equipment you are agreeing to the following terms:

- I will only use a mobile phone in the staff room or office areas. I understand that mobile phones should not be used in public areas during normal school hours.
- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and MLE tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body and will be encrypted.
- I will not install any hardware or software without permission of the ICT leader
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.
- Images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.