Winnington Park Primary School and Nursery

Internet Safety and Acceptable Use, Social Networking and use of Mobile Phones Policy

Updated: September 2023

Review date: September 2025

*Amendment May 2024

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Winnington Park Primary & Nursery School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Winnington Park Primary & Nursery School.
- Assist school staff working with children to work safely and responsibly with the Internet and other 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.
- Have clear structures to deal with online abuse such as online bullying.
- 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, including online pornography, ignoring age ratings in games (exposure to violence associated with often derogatory language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Online bullying in all forms
- Identity theft, including 'frape' (hacking Facebook profiles), and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, using the Internet or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Extremism
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope:

This policy applies to all members of Winnington Park Primary & Nursery School community (including staff, students / pupils, volunteers,
parents / carers, visitors, community users) who have access to and are users of School's Computing systems, both in and out of Winnington Park Primary & Nursery School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Online bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011

Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for E-Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, • which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training • to carry out their E-Safety roles and to train other colleagues, • as relevant • To be aware of procedures to be followed in the event of a serious • e-safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer (in the event of not being the Head). • To ensure that there is a system in place to monitor and support • staff who carry out internal E-Safety procedures
• ICT Leader	• Takes day to day responsibility for E-Safety issues and has a • leading role in establishing and reviewing the school E-Safety • policies / documents • Promotes an awareness and commitment to Online safeguarding • throughout the school community • Ensures that E-Safety education is embedded across the • curriculum • Liaises with school Computing technical staff • To communicate regularly with SLT and the designated Online safety Governor / committee 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 E-Safety incident • To ensure that an E-Safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ◦ sharing of personal data ◦ access to illegal / inappropriate materials ◦ inappropriate on-line contact with adults / strangers ◦ potential or actual incidents of grooming • • online bullying and use of social media

Governors	• To ensure that the school follows all current E-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. Governors will receive regular • information about E-Safety incidents and monitoring reports through the Headteacher's report. A member of the Governing Body is the E-Safety Governor. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • Regular review with the E-Safety Co-ordinator / Officer • E-Safety incident logs, filtering / change control logs
ICT Leader	To oversee the delivery of the E-Safety element of the Computing curriculum

Network Manager	• To report any E-Safety related issues that arise, to the E-Safety coordinator.
	• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
	• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)
	• To ensure the security of the school IT system
	• To ensure that 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
	  • CWAC is informed of issues relating to the filtering applied by the LA.
	  • That he / she keeps up to date with the school's E-Safety policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
	  • that the use of the *network remote* access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
	• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
	• To keep up-to-date documentation of the school's online security and technical procedures
	• ☐To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected
	• ☐To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Teachers	• To embed E-Safety issues in all aspects of the curriculum and other school activities • To plan and effectively deliver the School's On-line safety • 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	• To read, understand and help promote the school's on-line safety policies and guidance • To read, understand, sign and adhere to the school staff • Acceptable Use Agreement / Policy • To be aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the E-Safety coordinator • To maintain an awareness of current E-Safety issues and • guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
• Pupils	• ☐Follow the expectations of the Home School Agreement • ☐Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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 know and understand school policy on the use of mobile • phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of • images and on cyber-bullying. • To understand the importance of adopting good E-Safety • practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
• Parents/Carers	• To support the school in promoting E-Safety • To consult with the school if they have any concerns about their children's use of technology

Pupil E-Safety curriculum

At the start of each ICT unit within the curriculum staff deliver an E-Safety lesson relevant to the skills and behaviours appropriate to their age and experience. They include the following objectives:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;

- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- [for older pupils] To understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] To understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives

Expected conduct

In this school, all users:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online bullying Staff
- Are responsible for reading the school's E-Safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices. Students/Pupils
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations Parents/Carers
- Should know and understand what the 'rules of appropriate use' 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, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in on-line safety within the school. The 'Incident Reporting Form' (see appendix A) is completed. The records are reviewed/audited and reported to the school's senior leaders and Governors.
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- Removal of internet access rights for a period of time, with a programme of intense internet safety/risks lessons is delivered.
- Internet access is closely monitored.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law. Also, with staff, if it is deemed necessary, the LADO will be contacted.

4. Managing the IT and Computing infrastructure

Internet access, security (virus protection) and filtering

This school:

- Uses the CWAC Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses LA approved systems for secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Works in partnership with the CWAC to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the School's virtual learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search , …..
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use / School's virtual learning environment is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the [*Headteacher / teacher / person responsible for filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not
- share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are
- responsible for keeping their password private.
- We require staff to use strong passwords including capital letters and symbols.

E-mail

This school

- Provides staff with an email account for their professional use.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- 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
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

Pupils:

- Pupils are introduced to, and use e-mail as part of the IT/Computing scheme of work.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff can only use the email on the school system and staff only use school email for professional purposes

- Staff know that e-mail sent to an external organisation must be written carefully, (and may require
- authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of chain letters is not permitted;
- All staff follow the Teachers' Professional Standards and Code of Conduct relating to e-safety.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with the statutory DfE guidelines for publications;
- 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;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address.
- 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;

Social networking

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of
- personal information.

Facebook

Winnington Park Primary School and Nursery's Facebook page is used to celebrate our school and to share information. We expect all use of the Facebook page to reflect the ethos and values of our school.

All users of our Facebook page are expected to adhere to the following set of rules which will be regularly published to remind users of our expectations.

1. Winnington Park Primary School and Nursery's Facebook page is for sharing information and celebrating school life.
2. Please ensure that your use of the Facebook page reflects our school ethos and values. Be respectful, kind and keep everyone safe.
3. Abusive or derogatory posts will not be tolerated.
4. Contact the school directly if you have any questions. We are unable to respond to private messages or comments.

We take the Safeguarding of our school community extremely seriously. There will be consequences for unacceptable behaviour online, which will be the following:

- The user will have a conversation with the headteacher about appropriate use of the school Facebook page and try to agree a way forward.

- We will report to the Chair of Governors and keep a written record of the incident.
- The Chair of Governors may decide it is appropriate to block the user from accessing the page.
- If the Chair of Governors needs to escalate matters further, they will inform the Local Authority, which may result in legal action being taken.

Personal mobile phones and mobile devices

Mobile phones brought into school are entirely at the staff member, student's & parents' 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.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The school actively discourages pupils to bring in their own mobile phones and they can only be brought into school because of an exceptional circumstance and on written request form the parents / carers.
- Staff members may use their phones during school break times. Visitors are asked to follow our instruction regarding use of mobile phone.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded.
  All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring Search and Confiscation guidance from DfE
  https://www.gov.uk/government/publications/searching-screening-and-confiscation

Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.

- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned 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 phones or mobile devices.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Students' use of personal devices

- The School **strongly advises** that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone. In this instance, the parents must inform the class teacher in writing, giving permission for the phone to be kept in school on that day.

Smart Watches (amendment May 2024)

Staff members may wear a smart watch in school and it is recognised that this may be visible on a staff member's wrist. Smart watches should be placed on 'silent mode' and messages, calls and notifications should not be looked at or responded to in the presence of children.

Children must not wear smart watches in school. The use of Smart Watches is not appropriate in school due to risks of loss and damage and of misuse in the same way as mobile phones or tablets.

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 school agreement form when their daughter / son joins the school;
- 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
- 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 use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-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 IT 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 identify of others and their location, such as house number, street name or school. ☐We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal
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. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. 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.

Acceptable Use Agreement: Computers/Devices/Internet

Digital technologies have become integral to the lives of children and young people, both within and outside of schools. These technologies provide powerful tools which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. The school and parents, cares and family members have a duty of care to protect children and ensure that internet use is responsible and safe.

*The school strongly recommends that children do not use social network sites with age restrictions as this may pose a risk to children. Social networks are not accessible on internal school devices.

Please complete and return to your child's class teacher

As the Parents/Carers/Family Members of

Child's name _____

Year group _____

Teacher _____

Acceptable Usage Agreement

As the Parents/Carers/Family Members of the above child(ren), I give permission for them to have access to the internet and to ICT systems at school.

I know that my child has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the school's internet safety and acceptable use policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety. I will ensure that I monitor my child's use of the internet (including social media) outside of school. I will approach school staff online or invite them to join social networks online.

Signed _____

Relationship to child _____

Signed _____

Relationship to child _____

Date _____

Acceptable ICT Use Agreement: All Staff and Governors

Rules for Responsible Computer and Internet Use

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, website, software, communication tools, equipment and systems.

☐ I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

☐ I will not reveal my password(s) to anyone.

☐ I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

☐ I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.

☐ I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.

☐ I will not engage in any online activity that may compromise my professional responsibilities.

☐ I will only use the approved email system(s) for any school business;

☐ I will only use the approved *communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.

☐ I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

☐ I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *Computing Lead / Headteacher*

☐ I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

☐ I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

☐ I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

☐ I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils, parents or staff and will not store any such images or videos at home.

☐ I will follow the school's policy on use of mobile phones / devices at school

☐ I will only use school approved equipment for any storage.

☐ I will use the school's website in accordance with school protocols.

☐ I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

☐ I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

☐ I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.

☐ I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

☐ I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

☐ I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to *senior member of staff / designated Child Protection lead*.

☐ I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / Safeguarding Lead* on their request.

☐ I will only use any LA system I have access to in accordance with their policies.

☐ *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

User Signature

I agree to abide by all the points above.
I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
I understand that failure to comply with this agreement could lead to disciplinary action.

Signature

Date

Full Name (printed)

Job title / Role

Authorised Signature

I approve this user to be set-up on the school systems relevant to their role

Signature_____

Full Name_____

Date_____

Online Safety Incident Log	
Date	
Person Involved	
Incident	

Action Taken	
Outcome	
Persons Notified	
Completed by:	