Branton Primary School
and
Nursery

Online Safety (E-safety) Policy

Adopted from NCC

Policy Location:	Review Completed:	Review Due:	Person Responsible:
On website and in main school office.	October 2025	October 2026	Emma Miller Academy Committee

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety leader

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on: November 2024
The implementation of this Online Safety policy will be monitored by the: Headteacher & DSL Deputy DSL and ICT lead Governors
Monitoring will take place at regular intervals: Once a year This will include: ● Staff sign acceptable use agreement annually ● Review relevance of online safety curriculum ● Staff training ● Online Safety flow chart shared annually
The Online Safety Policy will be reviewed: November 2025 or earlier if significant changes occur.
Should serious online safety incidents take place, the following external persons / agencies should DSL, LADO or Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering

  (Senso and fortinite)
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 cyber-bullying or other Online 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

The governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by them receiving regular information about online safety incidents and monitoring reports.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community with support of the ICT lead.
- The Headteacher and the deputy DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that relevant staff receive suitable training.
- The Headteacher ensures that there is a system in place to allow for monitoring and

support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles. This is provided through NCC support team.

Headteacher/ICT lead:

● Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents

● ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

● provides training and advice for staff

● liaises with school technical staff

● receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

Technical staff through NCC SLA ICT support:

The Technical Support Staff and subject leaders for Computing are responsible for ensuring:

● that the school's technical infrastructure is secure and is not open to misuse or malicious attack

● that the school meets required online safety technical requirements and any Local Authority Online Safety Policy/Guidance that may apply.

● that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

● that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

● that the use of the network, internet, Learning Platform, remote access and emails regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher; Online Safety Coordinator for investigation/ action/sanction

● that monitoring software/systems are implemented and updated

Teaching and Support Staff:

Are responsible for ensuring that:

● they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices

● they have read, understood and signed the Staff Acceptable Use Policy

● they report any suspected misuse or problem to the Headteacher, Senior Leadership Team or the Online Safety Coordinator for investigation, action and/or sanction
● all digital communications with pupils, parents/carers should be on a professional level and only carried out using official school systems
● online safety issues are embedded in all aspects of the curriculum and other activities
● pupils understand and follow the Online Safety Policy and acceptable use policies
● they monitor the use of digital technologies, mobile devices etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
● In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead and deputies:

Are trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
● sharing of personal data
● access to illegal / inappropriate materials
● inappropriate online contact with adults / strangers
● potential or actual incidents of grooming
● cyber-bullying

(It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the roles of Designated Safeguarding Lead and Online Safety Officer).

Pupils:

● are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
● need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
● will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting 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, if related to their membership of the school

Parents / Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, Whole School Dojos and the school website. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platforms and online pupil records

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is to be; broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PSHE lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are helped to understand the pupil Acceptable Use Agreement and encouraged

to adopt safe and responsible use both within and outside school.

- Staff are encouraged to act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, Dojo, website, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites on school website

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The ICT Coordinator will receive regular updates through attendance at external

training events and by reviewing guidance documents released by relevant organisations.

- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements outlined by NCC guidance.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All KS1 and KS2 users will be provided with a username and secure password for google suite and school 360.
- Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system are kept in a secure place by the school's business manager.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of guests (e.g. trainee teachers, supply teachers, visitors) onto the school systems whereby they are issued with a guest username and password and receive and sign a copy of the acceptable use policy.
- Staff who are issued a school ipad will sign the staff ipad loan agreement regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- Agreed procedures are in place (See Data Protection Policy) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Two step authentications is required by all uses.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users are made aware that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents /carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published by staff that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

See separate Data Protection Policy.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through

● Ensuring that personal information is not published

● Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

● Clear reporting guidance, including responsibilities, procedures and sanctions

● Risk assessment, including legal risk

School staff should ensure that:

● No reference should be made in social media to 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 author it

● Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

● A process for approving members of staff to manage social media accounts

● At least two members of staff to monitor the accounts

● A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse

● Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

● Personal communications are those made via personal social media accounts. In all cases,

where a personal account is used which associates itself with the school or impacts on the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

● Personal communications which do not refer to or impact upon the school are outside the scope of this policy

● Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

● The school permits reasonable and appropriate access to private social media sites

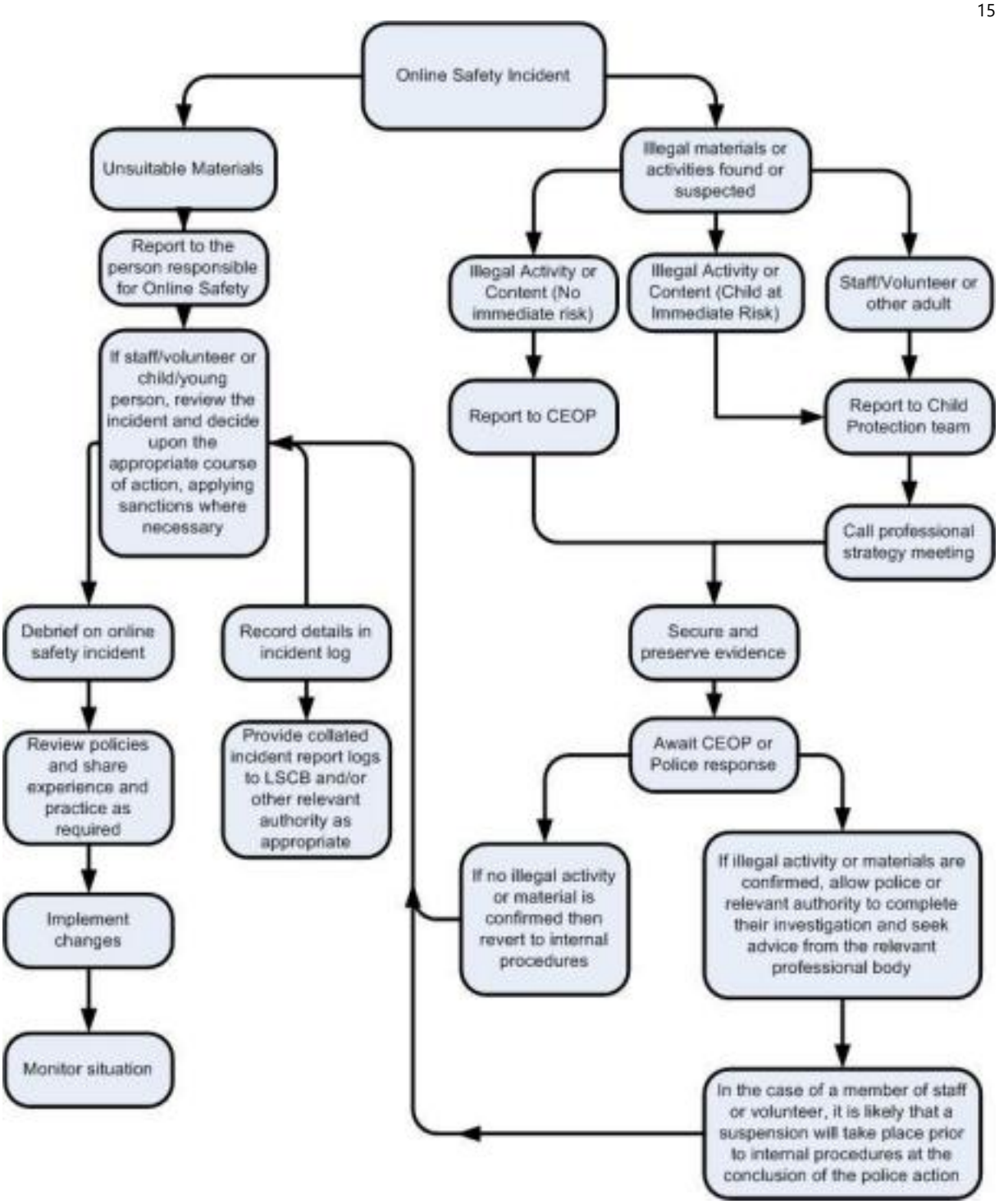
Monitoring of Public Social Media:

● As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school

● The school should effectively respond to social media comments made by others according to a defined process.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

● Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

● Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

● It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

● Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

● Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- o Internal response or discipline procedures
- o Involvement by Local Authority or national / local organisation (as relevant).
- o Police involvement and/or action

● If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- o incidents of ‘grooming’ behaviour
- **o** the sending of obscene materials to a child
- o adult material which potentially breaches the Obscene Publications Act
- o criminally racist material
- o promotion of terrorism or extremism
- o other criminal conduct, activity or materials

● Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Acceptable Use Agreement: Staff, Governors and Visitors Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Ms V Parr, Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I understand that, if a personal mobile device is used to access my school email account, it is my responsibility to ensure that the account cannot be accessed by other users of the device. School email accounts will always be logged out of when not in use.
- I will ensure that personal data (such as data held on MIS software) 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. Personal or sensitive data taken off site must be encrypted. If an email attachment is opened on a personal device and contains personal information, it must not be saved on that device.
- I will not install any hardware of software without permission of the ICT Technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- Images will not be stored on mobile devices including iPads and kindles.
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available, on request, to my Line Manager 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 into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies. ➢ I understand this forms part of the terms and conditions set out in my contract of employment and that if I deliberately breach this agreement, disciplinary action may be taken and police contacted if necessary.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……..(printed) Job title . . . . . .