TERRA NOVA
SCHOOL

Online Safety Policy

This policy applies to all sections of the School, including the Early Years Foundation Stage (EYFS)

Reviewed: May 2025

Next review: May 2026

Development, Monitoring & Review of this Policy

This online safety policy has been developed and reviewed by the Online Safety Group made up of:

- Online Safety Lead (also the Designated Safeguarding Lead)
- Network Manager
- Head
- Assistant Head Academic / Curriculum Lead Computer Science
- Safeguarding Governor

Consultation with the whole school community will take place through a range of formal and informal meetings when reviewing this policy.

Schedule for Development, Monitoring & Review

The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or significant incidents that have taken place.

The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at termly meetings of the Safeguarding Committee.

The school will monitor the impact of the policy using:

- Logs of reported incidents (via CPOMS)
- Monitoring logs of internet activity/filtering
- Internal monitoring data for network activity
- Periodic surveys/questionnaires of pupils, parents/carers, and staff.

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 digital technology systems, both in and out of school, including in the Early Years Foundation Stage (EYFS).

The Education and Inspections Act 2006 empowers Headteachers/Principals 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 online-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 community. 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 may be taken over issues covered by the School's 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/guardians 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.

Governing Body

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 the Governors receiving regular information about online safety incidents and monitoring reports. The Safeguarding Governor role includes Online Safety governance which will include:

- regular meetings with the Online Safety Lead / Designated Safeguarding Lead
- reviewing minutes or proceedings of meetings of the Online Safety Group via the termly Safeguarding committee meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to members of the wider Governing Body as necessary and appropriate.

Head and Senior Leaders

- The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead / Designated Safeguarding Lead;
- The Head and at least one other member of the Senior Leadership Team (usually the Deputy Head) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff;
- The Head is ultimately responsible for ensuring that the Online Safety Lead/DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- The Head shall be updated regularly on matters relating to online safety, including reports of incidents, via weekly meetings of the Senior Leadership Team.

Designated Safeguarding Lead

- The DSL is the school's Online Safety Lead, and assumes day-to-day responsibility for matters of online safety on behalf of the Head, as well as leading on the establishment, review and embedding of the school online safety policy;
- The DSL shall lead the Online Safety Group and ensure the Safeguarding Governor receives regular updates on matters relating to to online safety;
- The DSL ensures that there is a system in place to allow for support of those in school who carry out the internal online safety monitoring role;
- The DSL ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- The DSL provides periodic training for staff on matters relating to online safety, both within and beyond school, as well as being a source of advice for staff;
- The DSL liaises with the Local Authority;
- The DSL works closely with the school Network Manager;
- The DSL receives reports of online safety incidents and maintains a log of serious incidents to inform future online safety developments;
- The DSL meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering control logs;

- The DSL reports regularly to the Senior Leadership Team on all matters of safeguarding at the school, including online safety;
- The DSL shall receive training 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 on-line contact with adults/strangers
    - potential or actual incidents of grooming
    - online-bullying.

Network Manager

The Network Manager has technical responsibilities and is 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 technical requirements to maintain appropriate online safety in line with any Local or Statutory guidance;
- that users may only access the networks and devices through a properly enforced password protection policy;
- the filtering procedures as outline in this policy are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action;
- that monitoring software/systems are implemented and updated as agreed with the Online Safety Group.

All Staff

All staff employed by Terra Nova have a responsibility to safeguard children in the school's care, including in matters of online safety. It is expected of all staff that:

- they have an up to date awareness of online safety matters and of the school online safety policy and practices;
- they have read, understood and signed the staff acceptable use policy/agreement;
- they report any suspected misuse or problem to the DSL for investigation and action;
- 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 are helped to understand and follow the Online Safety Policy and acceptable use policies;
- pupils are supported to develop a good and age-appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras, 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.

Pupils

It is expected that all pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use policy;
- have a good and age-appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to have an age appropriate knowledge and understanding of policies on the use of mobile devices and digital cameras, the taking/use of images and on online-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

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents are responsible for:

- ensuring that their child has read and understood the relevant Acceptable Use Policy when it is issued to their child;
- discussing online safety concerns with their child, showing an interest in how they are using technology and encouraging them to behave safely and responsibly when using technology;
- consulting with the school if they have any concerns about their child's use of technology.

The school will take every opportunity to help parents understand online safety issues through newsletters and bulletins, letters, TN Talks, website, social media and information about national and local online safety campaigns and literature. Parents are 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 Platform and on-line pupil records,
- their children's personal devices in the school.

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school systems.

Education and Training

Education of Pupils

The education of pupils in online safety and digital literacy is 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 and Digital Citizenship is taught from EYFS through to Year 8. This is delivered by class teachers in EYFS and Pre Prep, and through Computer Science and PSHEE in the Prep School. Topics covered include staying safe online, online relationships, online bullying, wellbeing, social media, privacy and security. The

curriculum is broad, relevant and provides progression, with opportunities for creative activities. Teaching staff reinforce online safety messages across the curriculum and this is reviewed by the Online Safety Group.

Key online safety messages are also reinforced as part of a planned programme of assemblies and form/class time activities. Pupils are supported in building resilience to radicalisation by providing a safe and age-appropriate environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Pupils are helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.

Education of Parents

The school recognises that parents are not necessarily professional educators, and may have a limited understanding of online safety risks and issues. However, parents continue to play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may be unaware of how children and young people may come across potentially harmful and inappropriate material on the internet, and may be similarly unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and guardians through:

- Signposting to online safety information in letters, bulletins and on the school website and social media;
- Parent talks and workshops, such as TN Talks;
- Promotion of national and local events and campaigns such as Safer Internet Day;
- Links to relevant websites for parent information.

Training of Staff/Volunteers

All new staff receive online safety training as part of their induction process and safeguarding training so that they understand the school's Online Safety Policy and Acceptable Use Agreements. Staff will receive updates and further training from the Online Safety Lead/DSL or other members of the Online Safety Group as necessary, for example when new technologies, risks or resources are identified. Staff also participate in an Educare Online Safety training module as part of a rolling cycle of e-training. If staff identify further online safety training needs, the Online Safety Group will be notified to provide relevant training, advice or guidance as necessary.

Training of Governors

Where possible governors involved in online safety, safeguarding or technology will participate in the annual safeguarding training which includes online safety training in addition to completing the Educare Online Safety training module.

Updates and specific training when required will be provided to governors by the Online Safety Coordinator/DSL.

Technical

Network and access

The school's Network Manager is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are

implemented. The school's technical systems will be managed in ways that ensure that the school meets recommended technical requirements. The DSL and Network Manager will audit the safety and security of school technical systems annually and report to the Online Safety Group.

Servers, wireless systems and cabling are securely located and physical is access restricted. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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 devices are protected by up to date virus software. All users have clearly defined access rights to school technical systems and devices. Pupil and Staff devices on the school network are prevented from installing software.

The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Password security

The "master/administrator" passwords for the school systems, used by the Network Manager are also available to the Head and kept in a secure place.

All users in the Prep School will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames.

Passwords must not be shared with anyone. Users are responsible for the security of their username and password and must immediately report any suspicion or evidence that there has been a breach of security.

The school system requires passwords to be a minimum length and contain certain characters. User accounts will lock after three failed attempts to login.

Some systems such as iSAMS and CPOMS require additional username, password and two-factor authentication processes for enhanced security.

Filtering and Monitoring

Internet access via the school network is filtered for all users. The filtering of internet content is an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. The filtering system cannot however guarantee that all inappropriate content will be blocked as the content on the web changes dynamically and new technologies are constantly being developed. Parents and guardians are responsible for the filtering, security and parent controls of pupil's personal devices using personal data.

The school uses Smoothwall filtering system which is managed and monitored by the school Network Manager.

When a user tries to access a site that falls into the blocked categories/sites, they are unable to access the site and will see a message stating that the content has been blocked. The Network Manager is notified by

the filtering system of this occurrence and will follow up on any incidents of concern, when appropriate notifying the DSL.

The school actively monitors pupils' use of devices on the school network. Staff are trained in the use of classroom management monitoring systems and are able to make use of system functionality to monitor, record, lock and, if necessary, take control of pupils' devices in real-time during lessons. Monitoring of devices includes the automated delivery of alerts to the DSL and Network Manager according to pupil keystrokes where inappropriate or harmful phrases are used by children. Keystroke and phrase captures play an important part in understanding trends in potentially harmful communication, and are regularly analysed by the DSL.

Appropriate and proactive internet filtering ensures that children are safe from terrorist and extremist, inappropriate sexual, exploitative or other harmful material when accessing the internet. Filtering of extremist content is part of the school's wider safeguarding responsibility under the Prevent Duty.

Requests for particular websites to be made available or blocked are managed by the Network Manager and when appropriate are discussed with the DSL.

Staff use of mobile technologies (including BYOD)

The School Acceptable Use Policy for staff gives consideration to the use of Mobile technologies. 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 cloud based services such as email and data storage. Some staff are provided with school issued smartphones, laptops or computers which access the staff network and the internet. Users should not alter any security or network settings on any school issued devices. When a member of staff is leaving, HR will inform the Network Manager who will contact the staff member to arrange for return of the device.

In accordance with EYFS Statutory Framework, use of personal mobile devices in the EYFS is restricted as outlined in relevant guidance.

Staff may use their home or other internet access to securely access school systems. Staff may connect personal devices to the Staff network for reasonable use. The school network is filtered and monitored as outlined above. The school accepts no liability for damage or loss of staff personal devices. Use of staff personal devices are subject to the same rules as school devices as described in the Staff Acceptable Use Agreement and the Staff Handbook (Code of Conduct). The school reserves the right to confiscate staff personal devices if there is reason to believe the Acceptable Use Agreement has been breached.

Pupil use of mobile technologies (including BYOD)

Pupils in Years 1-3 access school-provided Chromebooks and iPads in their lessons. Pupils in Years 4-8 are asked to provide their own device. All devices should be clearly named. The school asks that Chromebooks are provided for pupils to use, as they are widely used alongside the Google Apps for Education platform that is used by the school. Upon enrolment, a pupil's Chromebook is given to the Network Manager who will register the device to the Google Admin panel during the first week of school and then return the device to the pupil. The school will purchase each pupil a Google licence which is used to domain manage the device (this £20 licence will be applied to the school bill). This in turn helps in the management of the device and the deployment of Apps.

Devices do not require a large hard drive or particularly high specification as most applications are run through a web browser as part of the Google Apps platform the school uses.

In the case of damage, parents and pupils are responsible for their own repairs. This includes loss of chargers. The school recommends that parents take out appropriate device insurance to protect against the possibility of accidental damage/loss.

Pupil use of school-provided and personal devices is subject to the Pupil Acceptable Use Policy which is made clear to all pupils upon joining the school and every September thereafter.

The Head or delegated authority has the right to examine and search pupil devices in the case of suspected misuse or in matters related to safeguarding. This is summarised in the Scope section of this document and is described in the school Behaviour Policy.

Use of digital and video images

Digital imagery of pupils

Written permission from parents or guardians is obtained before photographs of pupils are published on the school website/social media/local press. Permission is obtained as part of the Admissions process when joining the school via the 'Consent Form' and can be withdrawn at any time.

Images are used in a range of materials to promote Terra Nova School as a whole and to illustrate particular areas of school life. This includes (but is not limited to) advertisements and other publicity materials such as leaflets, brochures and posters, direct mail, books, newspapers, magazine articles, and online publications. Consent continues with no time limit. Images are retained in the school archive for possible future use. The school cannot withdraw images already published. Printed articles such as school handbooks will remain in use until updated.

When publishing digital/video images, staff should ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

In accordance with guidance from the Information Commissioner's Office, parents 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 or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images.

Pupils must not take, use, share, publish or distribute images of others without their permission. To do so will be considered a breach of the Acceptable Use agreement and will be dealt with under the school Behaviour Policy. Incidents of image sharing out of school on private devices may still be a matter for the school, where an incident affects or has the potential to affect pupils' school experience and personal wellbeing, or where the school has reason to believe that image sharing of an illegal nature has taken place.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs unless the express permission of the pupil and their parent/guardian has been obtained.

Permission to use full names is almost exclusively requested to celebrate pupils' successes, particularly where they have excelled in externally-run competitions or events, and would be considered an exceptional circumstance.

Creation and use of digital content in lessons and activities

Staff are responsible for explaining and monitoring safe and appropriate use and/or creation of digital content in lessons and activities. Where pupils and staff create digital content in lessons, these will only be created with permission of the participants; be of appropriate activities and of pupils wearing appropriate dress. Full names of participants must not be used either within the resource itself or within the file-name (or in accompanying text online). Digital content is usually uploaded to school file storage or school learning platforms (such as Google Classroom or Drive).

Staff may create digital video/images to support educational aims, and such content must always be stored inside the school network. The personal equipment of staff should not be used for such purposes without express permission from the Head.

Publishing digital content

The school maintains editorial responsibility for and copyright of any school-initiated website or learning platform content. The school maintains the integrity of the school website by ensuring that uploaded material is always moderated and that passwords are protected. The school has created a brand and as such neither pupils, parents nor staff should create online content that could be mistaken for being endorsed by the school, without prior permission from the Head.

School social media accounts are public so that prospective parents and pupils can view them. The school will obtain permission to publish content where someone else holds the copyright.

If someone posts offensive or inappropriate comments about the school, pupils or members of staff, they will be invited privately (via direct message rather than a public comment) to remove the post and to discuss their comments or concerns with the Head. Where the person is a current parent, they will be reminded of the school complaints procedure and the Terms & Conditions. Where the person is a current pupil, the issue will be dealt with under the school Behaviour Policy. Where the person is a staff member, the issue will be dealt with under disciplinary proceedings. The school will proactively monitor the internet for phrases relating to the school to correct misinformation and promote the school.

Data Protection

The school's data protection policy and procedures are described in the following documents:

- Data Protection Policy – Staff
- Data Retention Policy
- Privacy Notice
- Staff Privacy Notice

Communications

Any digital communication between staff and pupils or parents (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official school

systems. Personal email addresses, personal text messaging or social media must not be used for these communications.
Pupils must immediately report to a member of staff or parent the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils are educated about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies.

Staff should report to their line manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

The official school email service may be regarded as safe and secure, and is monitored. Users should be aware that email communications may be monitored.

Online meetings may be conducted via GoogleMeet, Zoom or Teams using audio only or audio and video. When in school, staff must ensure that they conduct the meetings in an appropriate space so that pupils cannot overhear or see the meeting.

Mobile Phones & Devices

Pupils are allowed to bring mobile phones to school in Years 5-8 however these must be handed in to the form tutor at the beginning of the school day and collected at the end of the day. Mobile phone or tablet use is not permitted at any time of the school day. The school accepts no liability for the damage or loss of devices. Pupils are able to make a phone call home if the need arises via main reception or the school nurse (if they are unwell in the surgery). Smart watches with WiFi enabled facilities or connectivity are not allowed in school.

Any phone or additional device that is seen or heard in school will be confiscated and handed to the Deputy Head. Following a confiscation, the child may be prohibited from bringing a device into school, either for a fixed period of time, or permanently.

On fixture days, when there is no end of day registration, phones may be handed over to the sports team who will arrange for their return.

Children will not have access to their phones during school hours, including on school trips and sports fixtures; if found accessing a phone or other device, this will be considered a breach of the policy and will result in the device being confiscated as outlined above.

Boarding

Flexi-boarders in Years 3-6 are not permitted to bring a mobile device into the boarding house. The Boarding team will ensure that there is an opportunity for flexi-boarders to telephone parents at home every evening, according to the wishes of the child.

Flexi-boarders in Years 7-8 are permitted to bring a mobile device with them to boarding, should they wish. Upon arrival in the boarding house, pupils must hand their mobile device to the boarding staff, who will store all devices securely. The school recognises the importance of education around the safe and sensible

use of mobile devices among pupils of this age, and pupils will have access to their device for a small amount of time each evening, should they wish. This will be supervised by a member of the boarding team.

All Weekly boarders, of any age, are permitted to bring a mobile device with them to boarding under the same terms as flexi-boarders in Years 7-8.

No personal devices are permitted beyond the Common Room areas on the first floor of the boarding house; should a child be found to have taken a mobile device up to the bedroom landings, this will be considered a serious breach of policy, and will be handled by the Head of Boarding in conjunction with the Deputy Head. In such instances, it is highly likely that a pupil will be prohibited from boarding for a period of time.

Working online

Staff – online teaching

- All contact with pupils and parents/guardians must be via school systems.
- Any online lessons will be conducted via the staff member's Google Classroom account.
- All lesson materials and prep are stored within the Google Classroom.
- Staff should ensure that any online lessons (whether pre-recorded or live) are undertaken in a neutral area and that nothing personal or inappropriate can be seen or heard in the background.
- Staff should be dressed appropriately.
- When using video, if a pupil is in nightwear, in bed, or has anything inappropriate around them, the staff member must terminate the call or remove the pupil from the online lesson and inform the Designated Safeguarding Lead.
- When delivering online lessons, if a person who is not a member of staff, pupil or parent/guardian (with prior agreement) joins, the teacher will remove them and report it to the Designated Safeguarding Lead.
- Any lesson that is required to be delivered in a 1:1 setting should be conducted using school platforms.

Pupils – remote learning

Pupils must log in to their Terra Nova Google Classroom. Pupils should ensure that any online lessons where they have their camera switched on are undertaken in a neutral area, at a desk and that nothing personal or inappropriate can be seen or heard in the background. Pupils must be dressed appropriately (nightwear must never be worn). Additional guidance is provided to pupils and parents in the event that remote learning is activated.

Social media

Social media (e.g. TikTok, Facebook, X, Instagram, Snapchat) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games and video sharing platforms such as YouTube have social media elements to them. The school recognises the numerous benefits and opportunities which a social media presence can offer, along with the associated risks, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents/guardians and when age-appropriate, children.

The school respects privacy and understands that staff and some older pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the School's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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.

Digital communications by staff must be professional and respectful at all times and in accordance with this policy and the Staff Handbook (Code of Conduct). Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school. Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account. Any such attempted contact should be reported to the Senior Leadership Team. Staff should also maintain professional boundaries with parents of current pupils and in cases where the member of staff is also a parent of a pupil at the school. Staff should not communicate with current parents about school business or matters concerning pupils via their personal social media accounts, as such communications should be via monitored School systems, including email and iSAMS. Staff members may have contact with parents for other reasons, often pre-dating a child's attendance at the School, and routine communication for matters not relating to school business is outside the scope of this policy. Staff are regularly encouraged to maintain the highest available privacy settings on their personal social media accounts, so that they are not easily found by pupils. Staff are expected to discuss with Leaders any relationship/association (in or out of school or online) that may have implications for the safeguarding of children in school.

The school will take appropriate action in the event of breaches of this policy. Where conduct is found to be unacceptable (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) this will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take further action.

Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing. Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

The school's education programme supports pupils to be safe and responsible users of social media when age-appropriate. The school has an active parent education programme which supports the safe and positive use of social media. This includes information in parent bulletins, on the school website and TN Talks.

Parents are welcome and encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent to remove the post and

invite them to discuss the issues in person. If necessary, the school will refer parents to the School's complaints procedures.

Dealing with online safety issues and incidents of misuse

The School may become aware of an online safety incident or that a user may have breached the Acceptable Use Policy through monitoring reports or from a report from a pupil, member of staff or parent.

If there are any safeguarding concerns, the Child Protection & Safeguarding Policy and associated procedures will be followed.

Illegal incidents

Where an illegal activity is found or suspected, a member of the Senior Leadership Team will report to the police immediately. Any devices and accounts involved must be secured. Where it is suspected that a device may contain images of Child Abuse, this must not, under any circumstances, be viewed by staff. If a police investigation takes place, this must be completed prior to any school investigation. Where the person involved is a member of staff/volunteer, the Head will contact the Local Authority Designated Officer (LADO) and the Child Protection & Safeguarding Policy will be followed. If the police confirm there is no illegal activity or material, the school will investigate the incident as described below.

The following non-exhaustive list shows which activities are illegal and would therefore always be dealt with as a disciplinary matter and reported to the police.

- Deliberately accessing, creating or sharing the following types of prohibited content:
    - Child sexual abuse images –the making, production or distribution of indecent images of children contrary to The Protection of Children Act 1978 (however, see Child Protection & Safeguarding Policy concerning children under 18 sharing images of themselves or others under 18)
    - Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003 (includes Sending of obscene materials to a child)
    - Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008
    - Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) contrary to the Public Order Act 1986

- Activities that might be classed as cyber-crime under the Computer Misuse Act:
    - Gaining unauthorised access to school networks, data and files, through the use of computers/devices
    - Creating or propagating computer viruses or other harmful files
    - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
    - Disabling/Impairing/Disrupting network functionality through the use of computers/devices
    - Using penetration testing equipment (without relevant permission)

- Any other criminal conduct, activity or materials

Incidents of misuse – staff

Any suspected staff misuse believed to constitute a breach of this policy, the Staff Acceptable Use Policy or Staff Code of Conduct will be investigated according to the Child Protection & Safeguarding policy and/or

Disciplinary & Dismissal Procedure. Staff personal devices may be confiscated by the Senior Leadership Team if a breach of this policy is suspected. Staff user accounts may be blocked by the Network Manager.

Incidents of misuse – pupils

Staff who become aware of a possible incident of misuse by a pupil will report it to the Online Safety Coordinator/DSL. Parents/guardians or pupils who become aware of a possible incident of misuse by a pupil should also report it to the Online Safety Coordinator/DSL.

The incident will be recorded on the Online Safety Log on CPOMS and where the incident is viewed as serious, parents/guardians will be informed.

Safeguarding of pupils is paramount during any investigation.

The incident will be investigated according to the school Behaviour Policy and/or Anti-Bullying Policy as relevant. Depending on the type of misuse, the class or form teacher, a Pastoral Lead teacher or a member of the safeguarding team will lead an investigation.

Incidents of mis-use may include:

- Unauthorised use of non-educational sites during lessons
- Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device
- Unauthorised/inappropriate use of social media/ messaging apps/personal email
- Allowing others to access school network by sharing username and passwords
- Using another pupil's or staff member's account
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or any other intentional acts to attempt to subvert the school's Filtering and Monitoring systems.

Pupil devices may be confiscated by the Head (or person authorised by the Head). Where internet sites need to be investigated to check whether the content is illegal or unacceptable, a device will be identified that is used for the entire procedure and that could be given to police if required.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Network Manager and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The School will decide if parents need to be informed if there is a risk that pupil data has been lost.

The School reserves the right to monitor equipment on our premises and to search any technology equipment, including personal equipment, when a breach of this policy is suspected. Confiscated devices may be searched by the Head (or authorised members of staff) and material deleted if there is no need to retain. Pupils may also be asked to delete material. Devices confiscated during the investigation will be returned at the earliest appropriate opportunity (unless removal of the device is to be part of the sanction).

Following the investigation, appropriate sanctions and support will be put in place for those involved. Sanctions for incidents of misuse may include removal of device access in school for a period of time, either alone or together with sanctions as described in the Behaviour policy. Where the Anti-Bullying Procedure is

used, an Anti-Bullying warning may be issued. As part of the school response to online safety incidents, pastoral or educational support may be provided.

Links to other organisations

The following links may provide helpful information on a range of online safety topics.

Safer Internet Centre – https://www.saferinternet.org.uk/

Childnet – http://www.childnet-int.org/

NSPCC - https://www.nspcc.org.uk/

Internet matters (helping parents keep children safe online) - https://www.internetmatters.org/

parentzone - https://parentzone.org.uk/

CEOP & CEOP Education Team - http://ceop.police.uk/ and https://www.thinkuknow.co.uk/