Inclusive Schools Trust

Lionwood Infant and Nursery School

Computing and Online Safety Policy

Signed: GHansell **on behalf of Trustees**

Date: 18.01.2022

Date: January 2022

Introduction

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. The internet is a part of everyday life for education, business and social interaction. Internet use is part of the statutory curriculum and a necessary tool for learning. The school has a duty to provide students with quality internet access as part of their learning experience. Students use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

Guidance to read in conjunction with:
DfE 'Keeping Children Safe in Education 2021'
Teaching and Online Safety (Government Document)
LIANS Remote Learning Policy
LIANS Behaviour Policy
LIANS Anti-Bullying Policy
LIANS Relationships and Health Education Policy
IST Cyberbullying Policy
IST Internet Social Network and Email Policy
IST Safeguarding Incorporating Child Protection Policy

Statement of Aims

- To provide a supportive, stimulating environment in which each pupil is enabled and encouraged to attain the highest standard of achievement of which he or she is capable.
- To ensure that the curriculum is broad and well balanced following all subjects in the National Curriculum.
- To ensure that the curriculum reflects the richness of our multi-cultural society.
- To value each pupil's contribution
- To encourage pupils to be aware of their behaviour and how it affects others
- To recognise that pupils have a variety of special needs and endeavour to provide appropriately for the needs of individuals
- To ensure staff and pupils know how to stay safe when using the internet.
- To foster and build on relationships with parents and Trustees.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, Trustees) who have access to and are users of school's digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers* to such extent as is reasonable, to regulate the behaviour of students when they are off the school 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. 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/relevant authorities of incidents of inappropriate Online Safety behaviour that take place out of school.

Responsibilities

Role	Key Responsibility
All Staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online 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 to the Designated Safeguarding Lead • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To plan and effectively deliver the School's Online 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 aware of legal issues relating to electronic content such as copyright laws where age appropriate.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: EYFS and KS1 parents / carers can sign on behalf of the pupils) • 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 taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies in school and out of 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 and Carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement (appendix) which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and promote the School's Pupil Acceptable Use Agreement with their children

	• To consult with the school if they have any concerns about their children's use of technology • Follow guidelines on the appropriate use of digital and video images taken at school events • Access to parents' sections of the website and learning platform (Class Dojo)
External Visitors and Trainee Teachers	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school
Trustees	• Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
Head/Head of School and Senior Leadership Team	• 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 Senior Leadership Team. • The Head and other members of the Senior Leadership Team 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. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority / MAT / other relevant body disciplinary procedures) • The Head/Senior Leaders will ensure 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 to those colleagues who take on important monitoring roles.

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 students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing /RHE /other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies (e.g. Safer Internet Day each February).
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

- Pupils should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit

Education – Parents/Carers

Parents play an essential role in the education of their children and in the monitoring and regulation of 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 will therefore seek to provide information and awareness to parents/carers through:

- Curriculum activities
- Letters, newsletters, School's Website/Twitter/Facebook/Class Dojo
- Parents/Carers evenings
- Events/campaigns e.g. Safer Internet Day

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- There are regular reviews and audits of the safety and security of school technical systems by way of regular system updates and backups.
- All users will have clearly defined access rights to school technical systems and devices. Users are made aware of this in the Acceptable Use Agreement.
- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the Head* or other nominated senior leader and kept in a secure place (currently held by JC Comtech). Admin credentials are changed regularly – users are encouraged to change passwords on a regular basis.
- School technical staff are 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

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the internet provider and relevant filtering policies rolled out via network.
- There is a clear process in place to deal with requests for filtering changes which must be approved by the Head.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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 include password protection, user level permissions, firewall, endpoint protection (Windows Defender) and 2FA on key accounts.
- The school infrastructure and individual workstations are protected by up-to-date virus software as a part of an agreement with JC Comtech and carried out in on-site visits.

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 the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that **the primary purpose of the use mobile / personal devices in a school context is educational** and should run on the school's Wi-Fi. Their use must be consistent with this policy and other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy and Acceptable Use Agreements. Teaching about the safe and appropriate use of mobile technologies should be taught as a part of the school's Online Safety education.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give further guidelines 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 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. 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 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/carers will be obtained before photographs of pupils are published on the school website/school's social media pages/local press and acceptable use of technology is agreed.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children at school events for their own personal use (as such use in 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 where possible. If personal equipment is used, once stored on school equipment, they MUST be deleted immediately.
- 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 on the website, other school's social media pages, or elsewhere 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.
- Pupil's work can only be published with the permission of the pupil and parents/carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

- It has a Data Protection Policy. This is managed through the Inclusive Schools Trust and all key documents and policy are available through their website.

- It has appointed a Data Protection Officer (DPO). This is managed through the Inclusive Schools Trust. The DPO is Caroline Mandilakis.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.

- The device must be password protected
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following list shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, 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
- Any digital communication between staff and pupils or parents/carers (email, school's social media pages, chat, blogs, learning platform etc.) must be professional in tone and content
- Whole class/group email addresses may be used at KS1
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, 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 without consent.
- 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 *s*chool or local authority
- 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 (Twitter, Facebook, Class Dojo) there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- 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 a 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

Monitoring of Public Social Media:

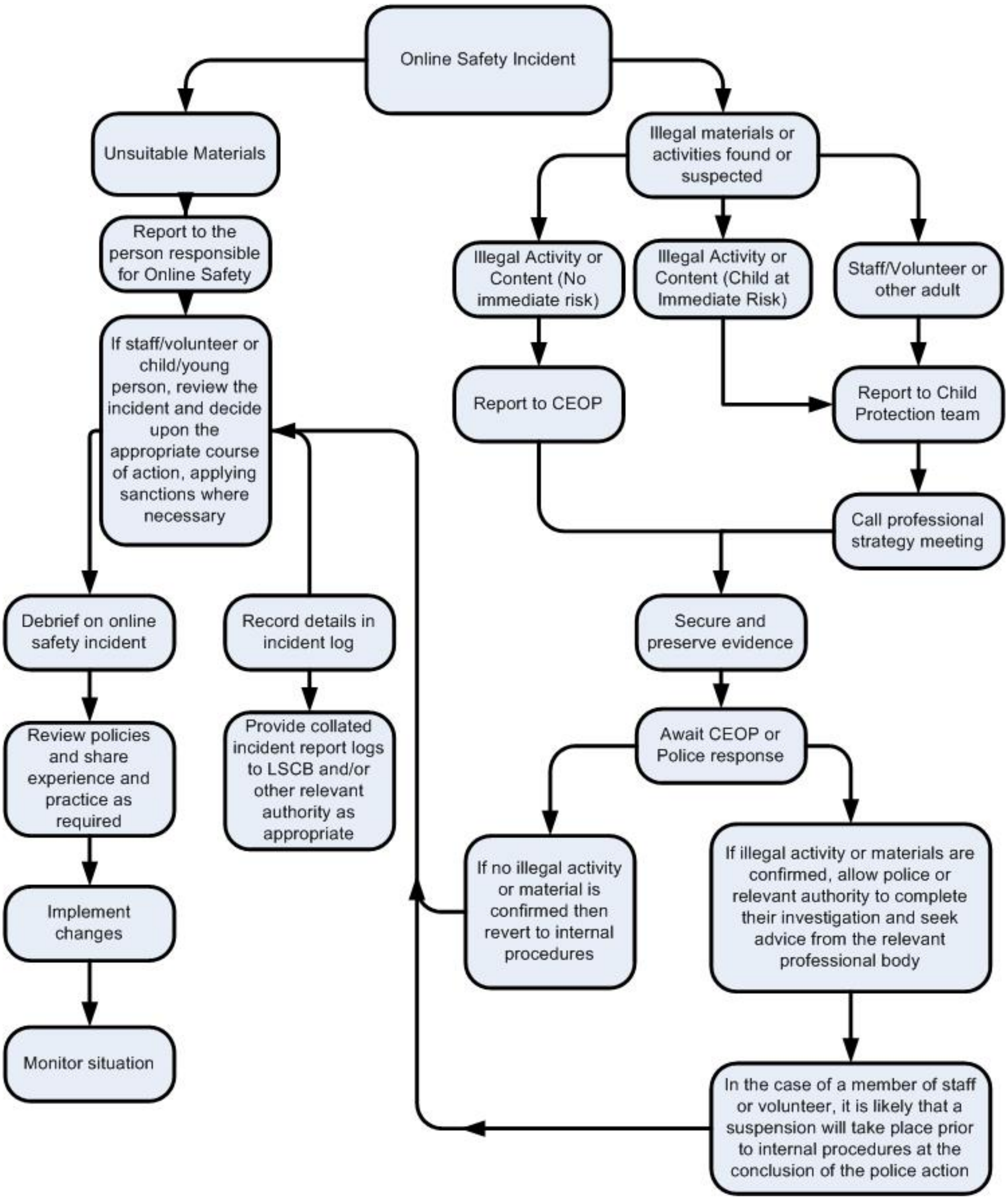
- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Head* and Senior Leadership Team to ensure compliance with the school policies.

Illegal Incidents

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



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:

- Where possible, more than one member of leadership staff will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The leaderships staff should conduct the procedure and complete a relevant incident log.
- 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:
    - Internal response or discipline procedures
    - Involvement by Local Authority and Trustees
    - 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:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - 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.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Any incidents will need to be reported to the Head* and Senior Leadership team. The police may also need to be involved.

* For clarity, at Inclusive Schools Trust, the term Head will incorporate the titles of Executive Head, Partnership Head and Head of School.

This policy will be reviewed every 2 years or sooner if the Computing curriculum is amended, for example in response to emerging themes, changing pupil needs or introduction of new legislation and guidance. **Every July it will be checked and reviewed by the Subject Leader and a member of the Senior Leadership Team** to ensure the appendix documents are current and ready for the new intake in September. The next full review date of this policy is currently set for **January 2024.**

Agreed: January 2022

To be reviewed: January 2024

Head of School's **signature** **Date: January 2022**

Appendix 1: Staff Acceptable Use Agreement

Lionwood Infant and Nursery School
Staff Acceptable Use Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head*.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal devices when used for school business.

- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by IST.

- If using my own mobile phone during school time to support planning, I will use the school's Wi-Fi account. I will not go onto social pages for example Facebook/Instagram.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will ensure that all school generated electronic communications are appropriate and compatible with my role.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head*. If in doubt I will seek clarification. This includes taking data off site.

- At school, I will not install any hardware or software without the permission of the Head*.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images will only be taken, stored and used for purposes in line with IST school policy (Internet, Social Networking and Email Use Policy) and with consent from parent/carers (Parent/Carer Acceptable Use Agreement). Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head*.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request by my Head*.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Leads (Hannah Kingsley, Sam Thorpe, Lucy Finnie)

I acknowledge that I have received a copy of the Computing and Online Policy.

Full name:……………………………………………………………………(printed)

Job title:…………………………………………………………………………………

Signature:……………………………………………………**Date:**……………………

* For clarity, at Inclusive Schools Trust, the term Head will incorporate the titles of Executive Head, Partnership Head and Head of School.

Appendix 2: Pupil Acceptable Use Agreement

Lionwood Infant and Nursery School
Pupil Acceptable Use Agreement
Foundation Stage and Key Stage One

To help me stay safe on the computer……

I will only use a computer when an adult tells me I can.

I will only use games or websites that a teacher or adult has told me to use.

I will not share my password.

I will take care of the computer, iPads and any other equipment.

I will tell an adult if I see something on the computer that makes me worried.

I will ask for help from a teacher or adult if I am unsure of what to do, or if I think I have done something wrong.

I know that if I break the rules I might not be allowed to use a computer or iPad

I have read through this agreement with my child and we agree to these safety measures.
Signed (child): ______________________
Signed (parent): ______________________
Date: ________

Appendix 3: Parent/Carer Acceptable Use Agreement

Lionwood Infant and Nursery School
Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside 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.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- Ensure robust safeguarding measures continue to be in effect during a period of remote learning.
- That school systems and pupils are protected from accidental or deliberate misuse that could put the security of the systems and pupils at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young children with regard to their online behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young children in their care.

Parents are requested to sign this permission form below to the show their support of the school in this important aspect of the school's work.

Permission Form

Pupil Name: ___________________

Singed Parent/Carer: _______________________

Date: _________

As the parent/carer of the above pupil, I give permission for child to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Pupil Acceptable Use Agreement with my child and that they have receives, or will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

Monitoring and Filtering Systems

I understand that the school will take very reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and 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 systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

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 safety.

Signed Parent/Carer: _______________

Date: _________

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff will use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons, and classroom displays.

Images may also be used to celebrate success through their publication in newsletters, Class Dojo, School Facebook, Twitter and website. Occasionally images might be used in the public media. Where an image is publically shared by any means, only your child's first name or initial will be used.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young children cannot be identified by the use of their names.

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.

Parents/carers are requested to sign the permission form below to agree for the school to take and use images of their child.

Digital/Video Images Permission Form

Pupil name: _________

Signed parent/carer: ______________

Date: ___________

As the parent/carer of the pupil above, I agree to the school taking digital/video images of my child. **Yes / No**

I agree to these images being used:

- To support learning activities **Yes / No**
- In publicity that reasonably celebrates success and promotes the work of the school **Yes/ No**
- On the school's website, newsletters, Class Dojo, Twitter and Facebook **Yes / No**
- I agree that if I take digital or video images at a school event which includes images of other children than my own, I will abide by these guidelines in my use of these images. **Yes / No**

Appendix 4: What do we do if…? Procedure

WHAT DO WE DO IF…
An inappropriate website is accessed unintentionally in school by a teacher or child?**

1. Play the situation down; don't make it into a drama.
2. Report to the child protection officer/ICT co-ordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (ICT Shared Solutions http://www.ict.norfolk.gov.uk/)
4. Inform Norfolk LA if necessary.

An inappropriate website is accessed intentionally by a child?**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Inform child protection officer/ICT co-ordinator and parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be. (Report to ICT Shared Solutions http://www.ict.norfolk.gov.uk/)
4. Inform Norfolk LA if necessary.

An adult uses School IT equipment inappropriately?**

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the Head* and ensure that there is no further access to the PC or laptop.
3. If the material is offensive, but not illegal, the Head* should then:

- Remove the PC to a secure place.
- Instigate an audit of all ICT equipment by the schools ICT providers, this could your technical support provider to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Take appropriate disciplinary action (contact Personnel/Human Resources).
- Inform the Tust of the incident.

4. In an extreme case where the material is of an illegal nature:

- Contact the local police or CEOP and follow their advice.
- If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time?

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Record the incident in the cyber-bullying record held by school admin team.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the sender's e-mail service provider if persistent.
8. Inform the police if necessary.
9. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff?

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Record the incident in the cyber-bullying record held by the Child Protection Officer.
6. Inform LA e-safety officer.
7. The school may wish to consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child?

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Contact CEOP (http://www.ceop.gov.uk/).
3. Consider the involvement of police and social services.
4. Advise the child on how to terminate the communication and save all evidence.
5. Inform LA E-Safety officer.
6. Consider delivering a parent workshop for the school community.
7. All of the above incidences must be reported immediately to the Head teacher.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

* Term Head is used which applies to Executive Head, Head of School and Head of Teaching School.

** **Inappropriate use** includes accessing sites which would be inappropriate for the age of the person accessing it, or the location in which it is accessed. Sites that fall under this definition include, but are not limited to: those that promote the use of alcohol, tobacco, gambling, illicit drug use and illegal activities; violence and violent extremist views including acts of extreme cruelty against animals or persons; full or partial nudity, and graphic sex.

Appendix 5 – Table of changes

Date of change	Paragraphs affected	Summary of update
January 2022	All	New Policy adopted