Crest Infant & Nursery School

Online Safety Policy

Person Responsible: Jane Shields
Date of Policy: October 2019
Date of next review: October 2022 (or in light of any changes in safeguarding legislation)

This policy forms part of Crest Infant & Nursery School's Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

CONTENTS

1. Introduction and Overview

This policy must be read in conjunction with the Keeping Children Safe in Education 2019 document guidance on online safety including Annex C.

Rationale

The purpose of this policy is to demonstrate how the school educates its community in order to safeguard as well as educate for a technological world. The policy aims to:

- Set out the key principles expected of all members of the school community at Crest Infant and Nursery School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff
- Assist school staff working with children to work safely and responsibly when usint the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures for dealing with online abuse such as online bullying (noting that these need to be cross-referenced with other school policies, particularly those relating to behaviour and safeguarding).
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

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

Content

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

Contact

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

Conduct

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

Scope

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

Roles and Responsibilities

Role	Key responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, inline with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a safeguarding 'culture', ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring the school's provision follows best practice in informaiton handling • To ensure the school uses apporpriate IT sysstems and services including filtered Internet Service i.e Atomwide services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' are undertaken to the curriculum meets the needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the online safety co-ordinator • To ensure there is a system in place to monitor and support staff who carry out internal online safety procedures e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure staff members are fully aware of legal issues relating to electronic content such as copyright laws • To ensure the school website includes relevant and statutory information
Online Safety Co-ordinator (Designated Safeguardiong Lead)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote and awareness and commitment to online safety througout the school community • Ensure that online safety education is embedded within the curriculum • Liaiase with school techinical staff where apporpriate • Communicate regularly with SLT and the designated safeguarding governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys/pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Keeps up to date with online safety issues and legislation, and be aware of the potential for serious child protection concerns
Safeguarding link Governor/Governing Body	• To ensure that the school has in place policies and practices to keep children and staff safe online • To approve the Online Safety Policy and review the effectiveness of this policy

	• To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety governor will include: regular reviews with the online safety co-ordinator
Computing Curriculum Lead	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/IT Technician	• To report online safety related issues that come to their attention to the Online Safety Co-ordinator • To manage the school's computer systems, ensuring -school policies are stricly adhered to -systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) -access controls/encryption exist to protect personal and sensitive information held on school-owned devices -the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and any online platforms are regularly monitored and that any mis-use/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate back up procedures and disaster recovery plans ar in place • To keep documentation of the school's online security and technical procedures up to date
Data and Information (Asset Owners) Manager (IAOs)	• To ensure the data they manage is accurate and current (and in line with GDPR) • Ensure best practice in information management i.e. have appropriate access controls in place, that data is used, transferred and deleted in line with data protection requirements • The school must be registered with the Information Commissioner
Atomwide nominated contacts	• To ensure all Atomwide services are managed on behalf of the school following data handling procedures as relevant
Teaching staff (including TAs)	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) • To ensure pupils are fully aware of research skills (and are fully aware of legal issues relating to electronic content such as copyright laws)
All staff, volunteers, contractors (where relevant)	• To read, understand, sign and adhere to the school Staff Acceptable Use Policy and understand any updates annually. The AUP is signed by new staff on induction • To report any suspected misuse or problem to the online safety co-ordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit Strategy** At the end of the period of employment/volunteering any equipment or devices loaned by the school must be returned. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with the line manager and technicial on the last day of employment to log-in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually

	• To understand the importance of telling an adult if they come across anything they feel uncomfortable with when using online technology • To know what action to take if they or someon they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy is relevant to their actions outside of school as well • To contribute to any 'pupil voice'/surveys which gather information about their online experiences
Parents/Carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/children • To consult with the school if they have any concerns about their child's use of technology • To support the school in promoting online safety and endorse the Parent's Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups or individuals	Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within the school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology

Communication

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

- Policy to be sent to all staff to read and comment on prior to being ratified by the governing body
- Policy to be posted on the school website and shared area
- Policy to be part of the school induction pack for new staff
- Acceptable Use agreements are discussed with staff and pupils at the start of each year
- Acceptable Use agreements to be issued to the whole school community on entry to the school

Handling Incidents

- The school will take all reasonable precautions to ensure online safety
- Staff and pupils are given information about infringements in use and possible sanctions
- The Online Safety Co-ordinator acts as first point of contact for any incident
- Any suspected online risk or infringement is reported to the Online Safety Co-ordinator as soon as possible and on the same day
- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure
- Any complaint about staff misuse will be referred to the Headteacher (or to the Chair of Governors if the complaint is about the Headteacher. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures. All online safeguarding complaints and incidents will be recorded by the school, including any actions taken
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

Review and Monitoring

The Online Safety Policy is referenced in other school policies e.g. Safeguarding, Child Protection, Anti-Bullying/Peer on Peer Abuse, Computing.

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

2. Education and Curriculum

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 88-90 of the KCSIE 2019 document which suggests resources that could support schools and colleges i.e:

• Teaching Online Safety In Schools - DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

• The UKCIS publication "Education for a Connected World Framework" The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.

Pupil online safety curriculum

This school:

- has clear, progressive online safety education programmes as part of the Computing curriculum/PSHE and other curriculum areas as relevant.
- ensures curricular planning for online safety is age appropriate
- will regularly remind pupils about their responsibilities through the Pupil Acceptable use Agreement;
- ensures staff members are aware of their responsibility to model safe and responsible behaviour in their own use of technology e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

As an infant school our children only use IT when supervised. Our rules are based on the SMART principle and form the basis of our Pupil Acceptable Use Agreement. Each class displays a set of rules at an age appropriate level.

The rules comprise of staying **S**afe, not giving out personal information on the web i.e. name, phone number, address, school name; never to **m**eet anyone you have met online, not to **a**ccept new friends without checking; make sure information you find is **r**eliable and to **t**ell the teacher/TA/parent if something makes you feel uncomfortable or worried.

Staff and Governor Training

This school:

- ensures staff members receive regular training on online safety issues as part of safeguarding training and also training on the school's online safety education programme
- provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent Awareness and Training

This school:

- provides updates for parents which includes tips for online safety in newsletters
- will arrange a rolling programme of online safety advice, guidance and training for parents

3. Expected Conduct and Incident Management

Expected conduct
In this school, all users:

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

Staff, volunteers and contractors

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

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

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

4. Managing IT and Communication System
Internet access, security (virus protection) and filtering

This school:

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

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the Atomwide USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the network manager is up-to-date with Atomwide services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Ensures pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted and only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Ensures our wireless network has been secured to appropriate standards suitable for educational use;
- Ensures all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password Policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, Atomwide USO admin site, twice a year.

E-mail

This school

- Provides staff with an email account for their professional use.
- We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

We use a number of Atomwide provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

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

Staff:

- Staff will use Atomwide e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

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

Cloud Environments

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

Social networking

Staff, Volunteers and Contractors

- Staff members are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupils use on a personal basis or to open up their own spaces to their pupils.

School staff will ensure that in private use:

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

Pupils:

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

Parents:

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

CCTV

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

5. Data security: Management Information System access and Data transfer
Strategic and operational practices

At this school:

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

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

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer
- We use the Atomwide USO AutoUpdate, for creation of online user accounts for access to broadband services and the Atomwide content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

6. Equipment and Digital Content

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

The school has a 'no mobile phone' policy and notices are clearly displayed in the main areas. Staff members will challenge parents or visitors who use their mobile phone inside the school premises.

- Mobile devices brought into school are entirely at the staff member, pupils & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- No personal devices should be used by staff to take photographs of children.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

Staff use of devices

- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned devices will not be used during teaching and learning periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff may use their phones during break times in the staffroom and other non-teaching spaces.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff will follow the guidelines set out in The Acceptable Use of Mobile Phones, Cameras and I-pads Policy when accessing School services, such as E-mail and calendars, via a school or personal mobile device.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- School owned devices will be accessed with a school account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

Pupils' use of personal devices

- No pupil should bring his or her personally owned device into school. Any device brought into school will be confiscated.

- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

Digital images and video
In this school:

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

This policy was reviewed as part of our School Improvement Plan 2018 – 2021
It was ratified by Governors on 10/10/18 and on 9/10/19

Date of next review: October 2022

Appendix A

ICT Acceptable Use Policy

(This policy is adapted from the model KCC & Medway Policy and is for Staff, Governors and Volunteers)

As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

- I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password; a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation, including GDPR.
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
    - Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent
- I will not keep or access professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. I will upload any work documents and files in a password protected environment e.g. the staff shared are on the school network system
- I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information
- I will respect copyright and intellectual property rights

- I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to a Designated Safeguarding Lead as soon as possible
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider (Paul Robinson) via Catherine Orr (School Business Manager), as soon as possible
- My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries, and will be transparent and open to scrutiny at all times.
    - All communication will take place via school approved communication channels such as a school provided email address, social media platforms or telephone numbers, and not via personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Headteacher
- I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Social Media policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school's staff code of conduct and the Law.
- I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with a Designated Safeguarding Lead and/or the Headteacher.
- I understand that my use of the school information systems, including any devices provided by the school, school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
- I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

NB: The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with CREST INFANT & NURSERY SCHOOL'S Acceptable Use Policy

Name: …… Signed: ……..... Date: …….

Accepted by: …….. Designation …….. Date: ……

Appendix B

Acceptable Use Agreement for Computing and Online safety

Pupils and Parents

These rules will help us to be fair to others and to keep everyone as safe as possible.

At Crest Infant & Nursery School we want you to enjoy using the computers, i-pads and Internet whilst in school and at home so we would like you to use the SMART rules.

It is very important I keep the SMART rules at home and at school. These are:

Safe
- **I will only go on the Internet when an adult is nearby**
- **I will never give out my password (even to my best friend)**
- **I will never give out my home address, full name or telephone number to anyone I don't know.**

Meet
- **I will never meet anyone I have chatted with online if I don't know them (even if they seem really nice). They are a STRANGER.**

Accept
- **I will think carefully before I click on or open something online (e.g. links, adverts, friend requests, photos)**

Rely
- **I understand that I cannot trust everything that is put online. I may need to ask a grown up to help me check information I find.**

Tell
- **I know I must tell an adult if I feel upset about something I see online.** This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or older brothers or sisters.

We have read these rules together and understand how important they are

Date: _____

Child's Name: _____ **Class:** _____

Parent's Name: _____ **Parent signature: _____**