Bringing out the best in everyone

NCBIS

Since 1978 New Cairo British International School

Name of Policy:	Online Safety Policy
Applicable to:	Whole school
Written by:	Tracy Connor, Kevin Rossall, Trevor Kearsley, Erasmus Dry
Contributors:	SLT, IT Director,
Approved on behalf of the ELT	
Effective date:	August 2019
Date of next review:	August 2021

Links to other relevant school policies

- Anti Bullying
- Child Protection - Voicing Concerns
- Child Protection and Safeguarding
- Staff Code of Conduct
- Behaviour
- Acceptable Use
- Staff disciplinary procedures
- Complaints procedure

NCBIS Mission Statement

To provide a learning environment that supports academic achievement whilst promoting personal growth through the attributes of the IB Learner profile, within a caring international community committed to the traditional values of honesty, courtesy, respect, integrity and fair play.

Purpose and Scope of Policy

Although our host country is not bound by Uk statutory law, as an International British School, this policy has been written taking into account UK statutory guidance 'Keeping Children Safe in Education' 2018, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018.

The purpose of this policy is to:

- Safeguard and protect all members of the NCBIS community online;
- Identify approaches to educate and raise awareness of online safety throughout the community;
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology;
- Identify clear procedures to use when responding to online safety concerns.

The policy is written to assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice. It aims to 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.

NCBIS identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

At NCBIS we believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing board, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services to the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Online safety is essentially about creating a safe environment when using IT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber-bullying, as well as detailing how we respond to e-safety issues when they emerge.

Roles and responsibilities

The Governing Board

The Board of Directors has overall responsibility for monitoring this policy and holding the principal to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL)

The board member who oversees online safety is The Chair Of The Board.

All board members will:

· Ensure that they have read and understand this policy.

· Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

· To approve the Online Safety Policy and review the effectiveness of the policy.

The principal

The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

· Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance.·

· To take overall responsibility for online safety provision.

· Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.

· To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.

· To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT Director and other staff, as necessary, to address any online safety issues or incidents
- 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
- Oversee any pupil surveys / pupil feedback on online safety issues

- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- To ensure that all reported online safety incidents are investigation and dealt with according to the incident response flow chart (appendix 3)

The IT Director

- The IT Directors is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
  This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To model safe, responsible and professional behaviours in their own use of technology.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

The text below is taken from the National Curriculum computing programmes of study.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In **Key Stage 3** pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4 & 5** will be taught to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- Understand the implications of their digital identity moving forward into higher education and careers.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, board members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Acceptable Use policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power as outlined under the UK Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Although we are not in the UK, NCBIS prides itself on adhering to UK standards for education and pastoral care.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure which is available on the school website.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. These can be found in the IT and acceptable use policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the Acceptable Use Policy.

Pupils and Staff using mobile devices in school

Any use of mobile devices in school by pupils or staff must be in line with the Acceptable Use Policy and Agreements.
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in a the IT and Acceptable Use Policy. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the IT director.

How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix

This policy will be reviewed annually by the DSLs. At every review, the policy will be shared with the governing board.

Appendix 1: online safety training needs – self-audit for staff

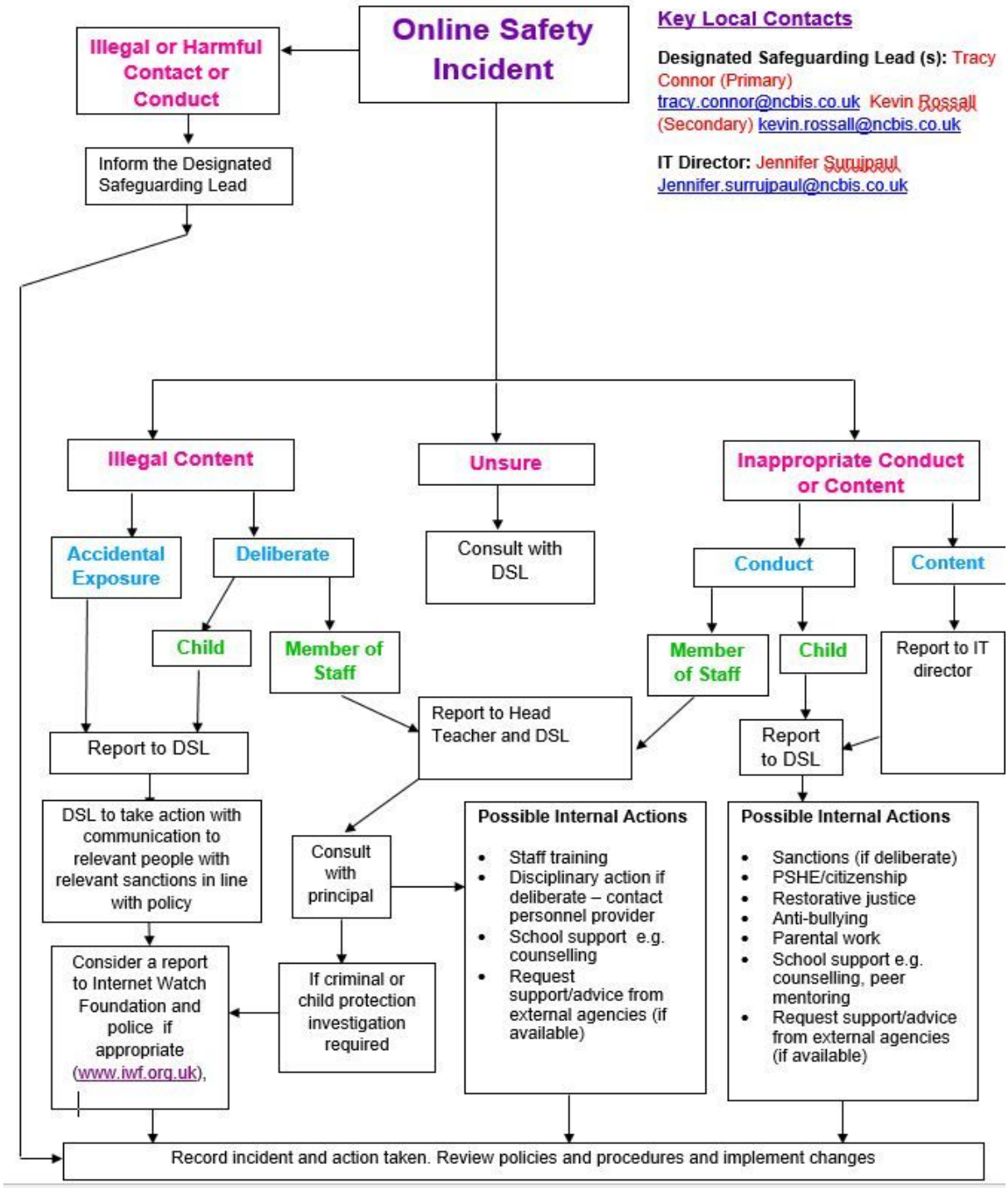
Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 2 Online Safety Log

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

Appendix 3


Online Safety Incident
Illegal or Harmful Contact or Conduct
Inform the Designated Safeguarding Lead
Key Local Contacts
Designated Safeguarding Lead (s): Tracy Connor (Primary) tracy.connor@ncbis.co.uk Kevin Rossall (Secondary) kevin.rossall@ncbis.co.uk
IT Director: Jennifer Surujpaul Jennifer.surujpaul@ncbis.co.uk
Illegal Content
Unsure
Inappropriate Conduct or Content
Accidental Exposure
Deliberate
Consult with DSL
Conduct
Content
Child
Member of Staff
Member of Staff
Child
Report to IT director
Report to DSL
Report to Head Teacher and DSL
Report to DSL
DSL to take action with communication to relevant people with relevant sanctions in line with policy
Consult with principal
Possible Internal Actions
Staff training
Disciplinary action if deliberate – contact personnel provider
School support e.g. counselling
Request support/advice from external agencies (if available)
Possible Internal Actions
Sanctions (if deliberate)
PSHE/citizenship
Restorative justice
Anti-bullying
Parental work
School support e.g. counselling, peer mentoring
Request support/advice from external agencies (if available)
Consider a report to Internet Watch Foundation and police if appropriate (www.iwf.org.uk),
If criminal or child protection investigation required
Record incident and action taken. Review policies and procedures and implement changes