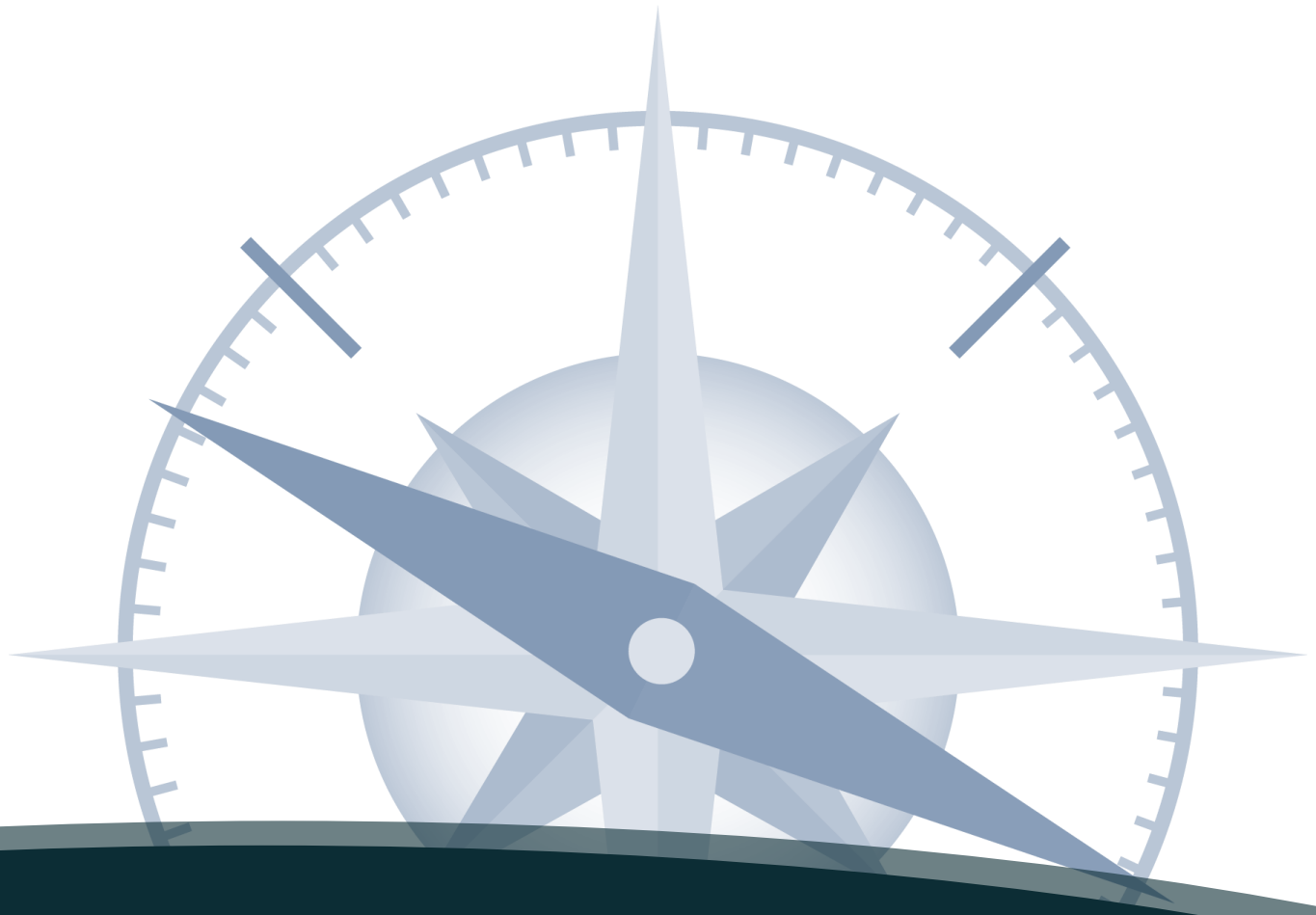

Online Safety Policy

Incorporating Acceptable Use of the Internet and Digital Technologies

THE COMPASS

PARTNERSHIP OF SCHOOLS

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

MAT – The Multi-academy Trust.

School – any school within the Trust.

Wider school community – pupils, all staff, governing body, parents

Introduction

Digital technology and the internet is an essential element in 21st century life for education and social interaction. The use of this technology enables access to worldwide resources and research materials, educational and cultural exchanges between children worldwide, online learning platforms for both staff and pupils, communication with support services, professional associations and colleagues, and the exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

In delivering the curriculum teachers need to plan to integrate the use of digital technologies to enrich learning activities. Effective and safe internet use is an essential life skill and the Compass Partnership of Schools is committed to ensuring children can develop this skill as safely as possible. The Compass Partnership of Schools believes that promoting a responsible attitude to the internet and digital technology in both our pupils, in partnership with parents, and our staff is vital to achieve this.

Safeguarding our children is at the heart of our values. The Keeping Children Safe in Education statutory guidance 2018 (Annex C) states that "an effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." Therefore, online safeguarding, known as Online Safety (previously E-Safety), is integrated, aligned and considered as part of each schools overarching safeguarding approach.

As this is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to our pupils or liability to the school.

This policy is available for anybody to read on the Compass Partnership of Schools website; upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Board of Trustees

The Board of Trustees is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:

    - keep up to date with emerging risks and threats through technology use.
    - receive regular updates from the head teacher with regard to training, identified risks and any incidents.
    - ensure all staff are taught about online safety as part of their regularly updated safeguarding training, and that this is considered as part of the school's overarching safeguarding approach.
    - ensure that children are taught about safeguarding, including online safety, through teaching and learning opportunities.
    - chair the Online Safety Committee

- Report regularly to Trustees regarding any online safety incidents and to confirm that all online safety pre-requisites are being observed.

Head Teacher

Reporting to the governing body, the head teacher has overall responsibility for safeguarding and online safety within our school. The day-to-day management of online safety will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The head teacher will ensure that:

- online safety training throughout the school is planned, up to date, appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents, and is integrated, aligned and considered as part of the overarching safeguarding approach.
- children are taught about safeguarding, including online safety, through teaching and learning opportunities.

- Designated Safeguarding Leads are able to understand the unique risks associated with online safety and are confident that they have up-to-date Online Safety training and up-to-date capability required to keep children safe whilst they are online at school.
- the designated Online Safety Officer(s) has had appropriate training in order to undertake the day to day duties.
- all online safety incidents are dealt with promptly and appropriately.

Online Safety Officer

The day-to-day duty of Online Safety Officer is devolved to Chloe Powell (Computing Lead Teacher)
The online safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the head teacher.
- Advise the head teacher, governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with MAT IT support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the MAT IT Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the head teacher and responsible governor to decide on what reports may be appropriate for viewing.

MAT IT Technical Support

The Trust Lead for IT will:

- Ensure the IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus and anti-malware software is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety officer and head teacher.

    - Passwords are applied correctly to all users *(Note: the specifics of the password policies, such as length and complexity, can be found in the Compass Data Protection Policy)*.
- Ensure IT Technical Support staff within each school, both in-house and bought-in, are adequately trained to manage the school's Online Safety technical solutions and that they are actively monitoring these systems.
- Regularly check that all search engines used by children are forced in "safe search" mode.
- Will support the schools Online Safety Officer in responding to incidents to ensure adequate measures are taken to reduce the risk of a recurrence.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the head teacher.
- Give pupils support in the use of digital technologies, including giving them advice on how to stay safe and to monitor their internet use.
- Any online safety incident is reported to the online safety officer (and an online safety incident report is made), or in his/her absence to the head teacher. If you are unsure the matter is to be raised with the Online Safety Officer or the head teacher to make a decision.
- The reporting flowcharts contained within this Online Safety policy are fully understood.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. The school will endeavour to keep parents up to date with new and emerging online safety risks and advise them on strategies they can deploy at home to keep their children safe online, through

parents training events, school newsletters, and the school website, and will involve parents in strategies to ensure that pupils are empowered online.

Parents must also understand that the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy (See Appendix 1) before any access can be granted to school ICT equipment or services.

Safe Use

The Compass Partnership Schools use a range of digital technology devices and online services, including PC's, laptops, tablets, social media platforms and cloud data storage facilities. In order to safeguard the student and in order to prevent loss of personal data, we employ the following safeguarding strategies:

Digital technology devices
staff will guide children in the safe use of all digital technology devices, including PCs, laptops, tablets, AV systems, digital cameras, etc. Safe usage includes physical safety (ie tablets should not be used with cracked or broken screens). If deemed necessary, a risk assessment should be performed on the usage of equipment.

Internet
Internet use will be granted to staff upon signing this Online Safety and the staff Acceptable Use Policy. Internet use will be granted pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Filtering and monitoring
Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the Online Safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs for Internet misuse.

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this policy, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network but is used in school or for school business).

Consent for monitoring is not a requirement. However, we are required by law (General Data Protection Regulations) to make all reasonable efforts to inform users that we are monitoring them. This is done via the staff and student Acceptable Use Policy (See Appendix 1).

Our internet filtering is provided as part of our LGFL internet service, using Netsweeper software, which is embedded into the school's firewall, to prevent unauthorised access to illegal and inappropriate websites. The Trust Lead for IT and each school's Online Safety Officer are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the head teacher.

Safe search tools will be enabled by default. This is managed by LGFL and should be regularly checked for operability by IT support staff.

Staff should be made aware that safe-search is not fool proof and that search engine usage should be monitored. If staff or children discover unsuitable content, the URL (address) and content must be reported to the online safety officer immediately, who will in turn report the incident to the head teacher and the internet filtering provider.

Email
Staff and pupil safe use of the Trust's email system is covered in the Trust Data Protection Policy.

Pupils may be permitted to use the school's email system on a case-by-case basis. Appropriate safeguards must be in place, such as a limited trusted recipient list.

The use of a non-MAT administered email system is prohibited from within school.

Our email filtering is provided as part of our LGFL "Staffmail" service (legacy email system) or as part of our Office 365 Tenancy. The specifics of the system can be found in the Trust Data Protection Policy.

Anti-virus/anti-malware
All capable devices will have anti-virus and/or anti-malware software. The specifics of our anti-virus/anti-malware systems can be found in the Trust Data Protection Policy.

Photos and videos
Digital media such as photos and videos are covered in the Compass Data Protection Policy.

Social Media
There are many social media services available; The Compass Partnership Schools is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.

The following social media services are permitted for use within The Compass Partnership Schools and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the online safety officer who will liaise with the head teacher and trust lead for IT. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and pupils on the school website.
- Twitter – used by designated members of staff within each school as a broadcast service (see below).
- Vimeo – used by designated members of staff within each school as a video broadcast service (see below)
- Showbie – used by staff, pupils and parents to share pupil work.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments should be disabled if possible or set to "moderated".
- All posted data must conform to copyright law; images, videos Are theand other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Cyber-bullying
The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Cyber bullying can differ from other forms of bullying:

- Through various media children can be cyber-bullied 24 hours a day
- People who cyber-bully may attempt to remain anonymous
- Anyone of any age can cyber-bully

- Some instances of cyber-bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient

We recognise that the best way to deal with cyber-bullying is to prevent it from happening in the first place. By embedding good, safe, respectful ICT practice into all our teaching and learning, incidents can be avoided.

We recognise we have a shared responsibility to prevent incidents of cyber bullying but the head teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies, in accordance with the behaviour and safeguarding policies.

Incidents of cyber-bullying should be recorded by the online safety officer as part of the online safety incident logging.

Understanding Cyber bullying
The school community is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance as part of their online safety training. Children are taught how to recognise cyber-bullying.

Radicalisation and Prevent Strategy
Please see the Compass Safeguarding and Prevent policies for more information.

Children with Additional Learning Needs
Schools in the Compass Partnership of Schools strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each child. Where a child has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Incidents
Any online safety incident is to be brought to the immediate attention of the online safety officer, or in his/her absence the head teacher. The online safety officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log.

The way an online safety incident is managed will depend on the severity of the incident, and the perpetrator(s) and victim(s). The online safety flow chart (see Appendix 2) should be followed.

Misuse and infringements
All members of the school community are aware of the procedures for reporting accidental access to inappropriate materials, through regular online safety training. The breach must be immediately reported to the online safety co-ordinator, who will log it in order that future risks to inappropriate materials can be minimised.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, and, depending on the seriousness of the offence: investigation by the Headteacher / LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

Users are made aware of sanctions relating to the misuse or misconduct through the Acceptable Use Policy, Staff Disciplinary Policy and Behaviour & Relationships Policy.

Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, The Compass Partnership Schools will have an annual programme of training as part of its overarching safeguarding strategy.

Online safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The online safety officer is responsible for recommending a programme of training and awareness for the school year to the head teacher and responsible governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the head teacher for further CPD.

Our Online Safety programme is facilitated through our Annual Safeguarding Training, Child Protection and Behaviour and Relationship policies, Subject Leader training, CPD for staff and PHSCE and Computing Curriculum and CEOP resources.

APPENDIX 1

Acceptable Use Agreements for staff and pupils

The Compass Partnership of Schools
Acceptable Use of Internet and Digital Technologies Staff Agreement

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are required to sign this Acceptable Use Agreement before being allowed access to these technologies.

- I know that I must only use school equipment in an appropriate manner and for professional uses, and that my usage is subject to monitoring and review.
- I understand that I should act as a role model to children and young people for the safe and responsible use of the internet and digital technologies.
- I understand that I should ensure children are accessing technology and online content appropriate for their age or stage.
- I understand that I need to obtain parental permission for children and young people before I or they can upload images (video or photographs) of themselves to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people.
- I have read the procedures for incidents of misuse or online safety in the online safety policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the designated online safety officer (or head teacher in their absence) in accordance with procedures listed in the online safety policy.
- I know who my designated online safety officer is.
- I understand the risks involved should I contact children and young people via personal technologies, including my personal e-mail, such as misinterpretation and allegations.
- I know I should use the school e-mail address and phones to contact parents.
- I know that I must not use the school ICT systems for personal use unless this has been agreed by the Headteacher.
- I know that I should ensure that devices I use in school have adequate anti-virus and/or anti-malware protection so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the General Data Protection Regulations (2018), have read the MAT Data Protection Policy and have checked I know what this involves.
- I will ensure that I keep all passwords secure and not disclose any security information without head teacher approval. If I feel someone inappropriate requests my password I will report this to my head teacher.
- I will adhere to copyright and intellectual property rights.
- I will only install and use hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system, such as tethering to a mobile phone or a mobile WIFI hotspot, is forbidden without head teacher approval. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been shown a copy of the Online Safety Policy to refer to about all online safety issues and procedures that I should follow. A copy can be found on the school website.

I have read, understood and agree with these Agreements as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…… Date……

Name (printed)……

Acceptable Use of Internet and Digital Technologies Pupil Agreement

Our Charter of Good Online Behaviour

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – that my school will monitor the websites I visit.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

Sample Letter to Parents:

Note: This is an example only; do not use word for word but tailor to your own requirements.

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorises websites in accordance with their content abd allows or denies these categories as appropriate.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school. In order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child, we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. If you have any questions or concerns, please contact dfcontact@deansfield.compassps.uk

Yours Sincerely
……

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

Signature - Date

Appendix 2: Online Safety Incident Reporting Log

To be completed as thoroughly as possible by the member of staff identifying the incident, with the Online Safety coordinator

Date(s) / time(s) of incident:

Duration of incident: (e.g. One off, a week, 6 months etc.)

Description of the online safety incident:
include detail of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.

Why do you have concerns about this incident?

Has the information been recorded and secured? Yes / No
If yes, where, when and what?

Has any computer or hardware been secured? Yes / No
If yes, where, when and what?

Who was involved and how do you know this?
Is there any evidence to suggest that false names/details have been given? Give full details of real names and email addresses etc where known.

How was the incident identified? e.g. by member of staff, informed by third party, etc.

What actions were taken, by whom and why? Give detail of agencies informed and contact person within those agencies

Name of person completing this form:

Signature:

Date:

Appendix 2:

Online Safety

This could be:
- Using another person's user name and password
- Accessing a banned or inappropriate website
- Using technology to upset or bully
- Downloading illegal content

Report to Online Safety Coordinator

1. Keep any evidence (screenshots, printouts, files)
2. Disable account(s)
3. Secure computer / Hardware

This may be:
- Any attempt to access child pornography
- Inciting hatred (e.g. racial, religious)
- Promoting illegal acts
- Extreme cyberbullying

Was illegal material or activity found or suspected?

If unsure, consult with Headteacher

YES

1. Inform the Police in the first instance
2. Confiscate any equipment and if on school network disable the account
3. Save all evidence, but do not view or copy. Pass the evidence to the police
4. If a member of STAFF is involved contact Greenwich LA Human Resources (HR) after informing the police
5. If a PUPIL is involved, after informing the police, contact parents and the LA Designated Officer

NO

Who did the incident involve?

STAFF

STAFF as an INSTIGATOR

If the member of staff has behaved in a way that has, or may have, harmed a child, OR committed a possible criminal offence, contact the LA Designated Officer.

If not, review the evidence and determine if the incident was deliberate or accidental. Decide on the most appropriate course of action, following disciplinary procedures if necessary.

STAFF as a VICTIM

Action will vary depending on whether the instigator was a parent, member of staff, or pupil. ***See separate advice.***

The HT or Chair of Governors should be the single point of contact to coordinate responses.

The member of staff may wish to take advice from their union.

PUPIL

PUPIL as an INSTIGATOR

Review incident and determine if others were involved. Decide on appropriate sanctions and/or support.

Inform parents of the details of the incident and its consequences for the perpetrator(s) and any victims.

In the case of a serious incident, report to the LA Designated Officer.

Review school procedure and policy.

PUPIL as a VICTIM

In-school support from:
- Class Teacher
- Class Team
- eSafety Coordinator
- Headteacher / SLT

as appropriate.

Inform parents of details of the incident and its consequences.

Consider whether it needs to be reported to the LA Designated Officer.

Review school procedure and policy.

Online Safety incident involving staff as a

Incident could be:
Using a Social Network to bully, intimidate or make hateful comments
Impersonation through the unauthorised use of logins and passwords

Parents/ carers as instigators

- Follow the steps below, as appropriate:
- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of discussions taking place online …
  - You want to discuss this...
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home School Agreement which clearly states …
- Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors
- You may also wish to send a letter to the parent

Other staff as instigators

- Follow the steps below, as appropriate:
- Contact Greenwich LA HR for initial advice and / or contact Schools eSafety Adviser **In all serious cases this is the first step.**
- If the police are not involved, contact the member of staff and request the offending material be removed immediately, (**in serious cases you may be advised not to discuss the incident with the staff member**)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff
- Informthe school's Governing Body (Governors need to be kept out of initial investigations so we are impartial if there is an appeal)
- Decide on the most appropriate course of action, following disciplinary procedures if necessary

Pupils as instigators

- Follow the steps below, as appropriate:
- Identify the pupils involved
- If the police are not involved, ask the pupil(s) to remove the offensive material. Refer to the signed Acceptable Use Agreement.
- If the perpetrator refuses to remove the material and is under 13 contact the Social Network, who will close the account
- Take appropriate actions in-line with school policies/ rules
- Inform parents / carers
- For serious incidents or further advice:
- Inform your Local Police Neighbourhood Team
- Contact the LA Anti-Bullying Adviser
- If the child is at risk talk to your school Child Protection Officer who may decide to contact the LA Designated Officer

Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	Online Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - pupils	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Pupils taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: **1 – 3 = Low Risk**
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: **The person who will action the risk assessment and recommend the mitigation to head teacher and Governing Body.**
Final decision rests with head teacher and Governing Bod

Risk Assessment

Risk No.	Risk
3	In certain circumstances, pupils will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; pupils will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
LIkelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	Online Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The Online Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school Online Safety education

	programme has already covered the safe and appropriate use of technology, pupils are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (head teacher) : **Signed (Governor) :**