Document last reviewed: November 2016

eSafety Policy

December 2016

Introduction and scope of the Policy

This policy seeks to formalise the management of eSafety risks, incidents, and education within the school. It should be read in conjunction with the school *Safeguarding and Child Protection Policy*, the GDST *Safeguarding Procedures* (which incorporate the staff *Code of Conduct*), the *IT Code of* Conduct and the *Anti-Bullying Policy*. These detail the steps that should be taken in any safeguarding issue whether it is mediated by technology or not.

While many of the risks around eSafety will be familiar, modern technologies have created a landscape of challenges and dangers that are still constantly changing. The continued development of systems and devices means that school leaders will need to be proactive and pragmatic in dealing with problems and threats as they emerge.

This eSafety Policy applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It applies to the whole school, including the Early Years Foundation Stage.

The nature of eSafety and GDST School Provision

Internet access is a feature of everyday life both in and out of school. Pupils and staff may use a number of networks and a range of devices in a single day and each may have different levels of access and capability.

Nevertheless, Northampton High School and the GDST believe that schools should be safe environments for learning. We judge the safeguarding of pupils both inside and outside school to be of the highest priority and therefore we adhere to the following principles:

- The highest standards of technological protection are included as part of school networks.
- Pupils are taught about eSafety in all its aspects as part of the curriculum, and eSafeguarding is seen as a responsibility of *all* staff.
- The school regards eSafety education as an important preparation for life.
- The school recognises that pupil and family information is sensitive and private. Data protection is regarded as a high priority.

1. Systems and Procedures

School Procedures and responsibilities

The school will identify a member of staff to co-ordinate eSafety. This may be the Designated Safeguarding Lead as the roles overlap. However, eSafety is seen as a whole-school issue, and different members of staff will have responsibilities as listed below.

Head	• Has overall responsibility for eSafety provision. • Has overall responsibility for data and data security (SIRO). • Ensures that the school uses the GDST filtered Internet Service. • Ensures that staff receive suitable training to carry out their eSafety roles and to train other colleagues, as relevant. • Is aware of the procedures to be followed in the event of a serious eSafety incident. • Receives regular monitoring reports from the eSafety Coordinator / Officer. • Ensures that there is a system in place to monitor and support staff who carry out internal eSafety procedures (e.g. network manager). • Oversees the staff Acceptable Use arrangements and takes appropriate action over staff who breach them.
eSafety Coordinator	• Takes day to day responsibility for eSafety issues and assumes a leading role in establishing and reviewing the school eSafety policies / documents. • Promotes an awareness and commitment to eSafeguarding throughout the school community. • Ensures that eSafety education is embedded across the curriculum • Liaises with school IT technical staff. • Facilitates training and advice for all staff. • Is the main point of contact for pupils, staff, volunteers and parents who have eSafety concerns. • Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident. • Ensures that an eSafety incident log is kept up to date. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering. • Liaises with relevant agencies. • Ensures that staff and pupils are regularly updated in eSafety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o cyber-bullying o sexting
Computing Curriculum Leader	• Oversees the delivery of the eSafety element of the Computing curriculum. • Liaises regularly with the eSafety coordinator.
Network Manager/technician	• Reports any eSafety related issues that arise, to the eSafety coordinator. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date).

	• Ensures the security of the school ICT system. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that the policy on web-filtering is applied and updated on a regular basis. • Ensures that GDST IT Department is informed of issues relating to filtering applied by the Trust. • Keeps up to date with the school's eSafety policy and technical information in order to carry out the eSafety role effectively and to inform and update others as relevant. • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school systems.
Data Manager	• Ensures that the school is compliant with all statutory requirements surrounding the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Ensures that GDST guidance and policies on the handling of information are implemented. (Guidance is available on the GDST staff intranet).
Teachers	• Embed eSafety issues in all aspects of the curriculum and other school activities. • Supervise, guide and monitor pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• Read, understand and help promote the school's eSafety policies and guidance. • Are aware of eSafety issues related to the use of mobile phones, cameras and hand held devices, monitor their use., and implement current school policies with regard to these devices. • Report any suspected misuse or problem to the eSafety coordinator. • Maintain an awareness of current eSafety issues and guidance, e. g. through CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
External groups	• Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Filtering and monitoring

All schools within the GDST are centrally provided with their data connections via a dedicated network. All incoming data are screened by an application that provides real-time filtering and protects both networks and users from Internet threats. It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to educational material from (for example) YouTube. The policy determining filtering is managed centrally, with different levels being applied depending on age group.

The filtering system produces a weekly report which identifies situations where pupils have tried to access sites which may give rise to concern. Monitoring can also be undertaken on a needs basis. For example, reports can be generated about the types of sites being accessed by users of the system and the number of times they have been requested.

There is also a centrally managed process for scanning email messages between staff and students for inappropriate language and behaviour. If there is an issue the HR department at Trust Office will be alerted and the matter is taken up with the school. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages can be retrieved by GDST IT.

The eSafety Coordinator keeps a log of all eSafety incidents in the school and shares this on a regular basis with the senior leadership team and school network manager. He/she also monitors the implementation of the eSafety Policy and ensures that its provisions are being implemented.

Acceptable Use Agreements and authorising internet access

Before using any school IT resource all staff members are required to read and sign an Acceptable Use Agreement (AUA) as part of their contract of employment. Staff have a dedicated log-on which requires them to use a strong password for access to the system. The first time they log-on, an automatic on-screen message reminds them about their responsibilities under the AUA and requires them to acknowledge this. Their response is then logged.

Differing versions of this agreement may be used to match the personal and professional roles of staff members. A copy of the agreement will be given to staff members for their reference. The AUA details how school equipment and connections may be used.

Pupils' Acceptable Use Agreements include eSafety guidance in the form of three age-appropriate leaflets or posters. Although not a legal contract, the agreements do set out what is expected by the school, and this guidance is shared with parents.

A separate register of when pupils were given (and agreed to abide by) the provisions of the agreement is kept for future reference with the pupil's records.

The school will keep a record of all staff and pupils who are granted Internet access through the individual usernames granted. The record will be kept up-to-date. (This will take account of changes such as a member of staff who has left the school or a pupil whose access has been withdrawn.)

Visitors to the school can be given access to the Internet by connecting to Visitor wireless. The filtering and monitoring systems apply as above. Access for visitors is provided under the general terms and conditions of the GDST, which prohibit the sending or receiving of materials which "are offensive, abusive, defamatory, obscene, or menacing" or which are illegal. The visitor signs a disclaimer which outlines restrictions and expectations of use.

Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the Internet for legitimate personal use (for example to contact a son's or daughter's school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in detail in the *Acceptable Use Agreement* and in the *Social Media Policy*, but will include:

- Keeping a proper professional distance e. g. not "friending" pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or emails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

Misuse of school systems

Because the staff *Acceptable Use Agreement* is part of the contract of employment, misuse is a disciplinary matter.

Pupil misuse (for example the sending of bullying messages to another pupil) may result in the withdrawal of facilities or further sanctions in line with the school's disciplinary policy.

Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further action depending on the nature of the misuse.

2. eSafety, Pupils, and Safeguarding

Teaching eSafety in School

The school curriculum includes lessons and activities in eSafety for all pupils.

The intention is to develop pupils' **awareness**, **resilience**, and **skills** in the wider electronic world. Pupils will explore issues such as:

- **Persuasion and reliability** (internet scams, phishing, unreliable information, radicalisation and extremism, etc.);
- **Personal information and safety** (sexting, social network information, personal images, etc.);
- **Sexual exploitation** (grooming, sexting, "offender not present" activities, etc.);
- **Online bullying** (text abuse, "trolling", etc.).

The activities are differentiated with regard to age.

The curriculum is varied and may comprise:

- staff-led skills sessions (e.g. How to configure *Facebook* privacy settings)
- whole-school assemblies led by older pupils, and other examples of peer mentoring
- discussion groups
- 'Safer Internet Day' activities
- formal lessons.

The teaching covers not only what the problems are, but how to deal with and avoid them. Wherever possible, we engage older pupils to share their experiences and advise others about personal safety and responsibility online.

These activities and lessons form part of the Computing/IT and PSHE schemes of work.

The eSafety Coordinator keeps up to date on emerging trends and alters the guidance and focus of the curriculum appropriately.

Guidance to pupils on using email and other messaging systems

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

As part of the *Acceptable Use Agreement*, pupils undertake never to send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students are reminded that the sending of abusive messages is illegal.

Particular concerns

Inappropriate material appearing on school computers

- Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting. They are encouraged to talk to their teacher. The teacher should report the incident to the eSafety Coordinator who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

- Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages. The eSafety Coordinator will be informed and an investigation begun initially with the help of the Network Manager.

Pupil reporting outside school

- Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that as well as talking to a teacher they can share this with their parents, and consider using the online **Report CEOP** button to make a report and ask for help.

Mobile data

- Whilst access to the internet using the GDST network will be subject to filtering and monitoring, the school is aware that many children will have unlimited and unrestricted access to the internet, for instance via 3G and 4G personal devices, both whilst in school and outside school. However, the AUA the pupils sign and the school's eSafety education cover the responsible use of IT in any situation, whether using the school's networks or not. The school's Mobile Device Policy also outlines sanctions that may be applied if students misuse devices while in school.

Staff training and updates

- All staff will have eSafety training included as part of their safeguarding induction to the school.
- All staff receive regular training in safeguarding pupils. eSafety is included as part of this. Staff members receive training in specific elements of eSafeguarding (e. g. self harm) and a broader update at least once a year.
- eSafety incidents and concerns are a standing item at staff briefings.

Reporting of eSafety concerns

The school takes reports concerning eSafety very seriously. The action taken depends on the nature of the concern raised.

All incidents that come to the attention of school staff should be notified to the eSafety Coordinator.

The eSafety Coordinator will ensure that pupils, parents, volunteers, and staff understand that they can contact them with concerns at any time.

Any incident that raises wider safeguarding questions will also be communicated to the Designated Safeguarding Lead(s) and action under the *Safeguarding Policy* and *Procedures* will be considered.

School Website

Advice, guidance, and links are available through the school's website for parents and pupils. This advice includes details of how to report a problem to the school, and which members of staff have responsibility for resolving a problem or taking issues further. The school will also look towards introducing an anonymous reporting system which will enable anyone with a concern to share it with the school easily and directly.

3. Risk Management – Everyday eSafety

Assessing risks

The school will take all reasonable precautions to ensure that users abide by the acceptable use rules and access only appropriate material.

The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use rules which are published for their protection.

Due to the international scale and linked nature of Internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff using IT equipment will mainly be covered by the provisions of the *Display Screen Equipment (DSE, Health and Safety) Regulations* 1992. Guidance, definitions, and requirements can be found on the Health and Safety section of the GDST staff intranet.

The use of DSE by pupils is not covered by the *Display Screen Equipment Regulations*. However, it is good practice to apply the requirements of the legislation to their workstations thus helping them to develop safe working practices. In particular, it is recommended that adjustable seats are provided at pupil workstations and they should be given guidance on appropriate work positions and routines.

If pupils are issued with laptops, tablets, etc. then a risk assessment must be completed and guidance on how to use them given safely. A template risk assessment and pupil advice sheet can be found on the GDST staff intranet Health and Safety Section.

The risk of the use of technology for radicalisation is dealt with in the policy for the promotion of British Values and prevention of radicalisation.

Use of mobile phones and cameras

In order to prevent allegations of inappropriate activities, including against EYFS staff, staff must not store images of pupils (taken in a school capacity) on any personal device.

Any images taken on personal devices must be downloaded to school or GDST systems as soon as reasonably possible and the personal copy permanently removed.

Staff must be careful to avoid taking any photos of pupils that could be construed as inappropriate and any photos that may inadvertently be seen as inappropriate should be destroyed.

Students are warned of the acceptable use of phones as cameras in the mobile device and IT acceptable use policies.

Publishing staff & pupil information and photographs

- **The school website**

The contact details on the website should be the school address, email and telephone number. Staff contact details might include a school email address. Pupils' personal information will not be published.

The Head has overall editorial responsibility and ensures that content is accurate and appropriate.

- **Publishing pupils' images and work on the web**
    - **Open / public sites**

Public sites could potentially be used to gather information and the locations of pupils. Written permission to publish photographs and work on websites will have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (e. g. to celebrate a prize) the following guidelines should be observed:

1. Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.
2. Photographs published on the website or elsewhere, that include pupils, will be selected carefully. Care will be taken when taking digital/video images that pupils are appropriately dressed.
    - **Closed/ Secure sites**

Pupils' images, video, and work can be made available to parents on secure areas of the web as long as the following measures are adhered to:

1. The parents/carer should have a secure log-on to view the information on their pupils.
2. Parents should be made aware that their child's images may be included in group work viewable by other parents/carers.

Using web sites with pupils

Pupils are often directed to Internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing digital world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- All sites are filtered via the "Fortinet" system to minimize the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, the minimum of identifiable personal information will be disclosed and only school emails will be used.
- The school will be as open as possible about the sites and software it uses, and it welcomes queries from parents who wish to raise concerns or understand more about the way that IT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be understood that potential problems or harm may not emerge until after the adoption of a technology.

The senior management of the school (including the eSafety Coordinator) will reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

Handling eSafety complaints

Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.

Any complaint about staff misuse must be referred to the Head.

For impartiality, investigations into IT misuse by school staff will be carried out by the GDSTs IT Security & Compliance Manager.

Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures.

Pupils and parents are informed of the school's complaints procedure.

Using non-School Equipment – "Bring Your Own Device"

Under some circumstances, teachers and pupils are now able to use their own equipment in school and connect to the available network. This is normally called "bring your own device" (BYOD).

Whether staff member or pupil, it is made clear to the user that the rules and expectations surrounding online behaviour remain in force regardless of the ownership of the equipment being used. The school's Mobile Device Policy covers this in more detail.

4. Communicating the Policy

Introducing the eSafety policy to children

- Versions of the eSafety/Acceptable Use rules are posted in all networked rooms and discussed with pupils as needed. The aim is to keep the policy familiar and fresh for pupils rather than treated as something which is only referred to at odd times.
- Pupils are made aware that network and Internet use is monitored.

Staff and the eSafety policy

- All staff will be given a copy of the eSafety Policy and its importance explained.
- They signed a copy of the Staff Acceptable Use agreement as part of the contract of employment.
- Staff should be aware that internet traffic and email can be monitored and traced to the individual user. Because of this, discretion and professional conduct are essential.

Communicating eSafety information to parents

- The school website gives information on eSafety and how the school can help.
- eSafety advice will be included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- The school holds eSafety events to brief parents about eSafety developments and policies; possibly as part of events such as 'Safer Internet Day'.
- Wider information events for parents will have eSafety items included in the programme.

eSafety - Sources of information and guidance

Compiled by John Wheeler, Educational Computing Consultant, for the GDST

Resources for pupils, parents, and teachers	
GDST Live My Digital http://www.gdst.net/article/introducing-live-my-digital-learning-about-digital-living-together	The videos look at the ways in which the internet and digital technology can be used positively by young people as well as identifying the potential issues they may face.
Think you know https://www. thinkuknow. co. uk/	A premier site for resources and activities across the age ranges. This is linked to CEOP and is still one of the best places to look for resources and guidance.
CBBC Stay Safe Pages http://www. bbc. co. uk/cbbc/topics/stay-safe	A collection of games, quizzes and activities about eSafety in general. Very visual and engaging.
Childnet International http://www. childnet. com/	One of the first organisations to promote internet safety. Their SMART rules are written into the GDST guidance for pupils. The site has lots of information and activities with more of a emphasis on Junior and infant pupils (eg Digi-Duck)
Digizen http://www. digizen. org/	A Childnet project about digital citizenship. Looking slightly out of date now, but with some useful ideas, activities, and videos.
Digital Literacy guidance and teaching materials **Professor Alan November** http://novemberlearning. com/educational-resources-for-educators/information-literacy-resources/	These invaluable resources can be used to teach young people • Not to believe everything that is on the web • How to check where information is coming from • How to "read" web resources Some useful links to other teaching and "spoof" sites such as the North West Tree Octopus.
Ten Tips for Using Facebook http://www. broadway-academy. co. uk/wp-content/uploads/2014/07/Facebook. pdf	This PDF resource is published by Broadway Academy in Birmingham. It offers safety tips and then reasons why they are a good idea. It would make a good starting point for a lesson with senior pupils.

Beat Bullying http://www. beatbullying. org/	

	An independent organisation that works inside and outside of schools to develop young people as cyber-mentors. These mentors then help more marginalised students cope with bullying issues.
NSPCC – Online safety http://www. nspcc. org. uk/help-and-advice/for-parents/onlineSafety/onlineSafety_wdh99554. html	Materials on a number of areas including sexting, and cyber bullying. Well worth a look.

Guidance and information for school managers, leaders and others.	
CEOP http://ceop. police. uk/	Child Exploitation and Online Protection Centre. Now a section of the National Crime Agency, CEOP is less active than in the past, but still a mainstay of training and resources.
Get Safe Online https://www. getsafeonline. org/	A good "expert" site part-funded by the UK Government which covers a wide range of issues from technical to social. Really comprehensive and a good place to think about the issues and get information.
UK Safer Internet Centre. http://www. saferinternet. org. uk/	This a site which amalgamates information and links from Childnet International, South West Grid for Learning, and the Internet Watch Foundation. This is where the UK Safer Internet Day is promoted and organised. Well worth a look.
London Grid for Learning http://www. lgfl. net/esafety/Pages/safeguarding. aspx	Although LGFL's main purpose is to link state schools across London, their eSafety resources are open to all and are quite exceptional. They include sample school policies, links to audit tools, and Ofsted expectations. Not everything is recent, so it is wise to pick and choose, but still excellent.
South West Grid for Learning http://www. swgfl. org. uk/home	Like the LGfL, this is one of the original broadband consortia for schools. However, they have developed a suite of audit tools and eSafety training services which schools can buy into or use by registering. The 360 Degree Safe audit is liked by a number of schools.
Internet Watch Foundation **https://www. iwf. org. uk/**	The industry organisation for the reporting and removal of UK based illegal and abusive material on the web. Contains a reporting form and guidance on various forms of content. It has no jurisdiction outside of the UK but will pass on information to appropriate authorities.
Digital Awareness UK **http://digitalawarenessuk. com/about/**	A company which uses young internet professionals to advise schools and pupils on their online presence.

Guidance with a more technical bias	
Microsoft Safety Center http://www. microsoft. com/en-gb/security/family-safety/default. aspx#Internet-use	This is a text-based list of things that families could/ should do online. A little obvious and worthy perhaps, but still sound and with links to Microsoft OS tools for taking control of access and denying unwanted sites.
Norton Anti- Virus blog /guidance http://community. norton. com/blogs/norton-protection-blog	Norton's blog, is more than an advertising vehicle and contains information on new scams and threats as they arise together with technical and non-technical ways to protect yourself.

Google Safety https://www. google. com/safetycenter/#home	This is a set of tools to try and make the most popular of search engines more family friendly. Amongst other things it sets out how to select "safe search" on a browser and then lock it. (However a personal test of "safe search" suggests that it cannot be totally effective. It isn't a panacea.)
OFCOM – Guidance on Parental Controls for Games Consoles http://consumers. ofcom. org. uk/internet/onlineSafety-and-security/parental-controls-for-games-consoles/	Very useful advice on internet-connectable devices and how they can be managed. They also have information on mobile phone usage. HOWEVER, beware of the links to a site called "Chatdanger" which is not information or education but now appears to be links to explicit chat sites.
Netlingo www. netlingo. com/emailsh. cfm	An online dictionary of "text chat" for decoding conversations. Often enlightening and sometimes verging on the poetic. . . The problem is that subgroups make and use acronyms all the time and they go in and out of fashion. What may be commonly understood in Sydenham may be unheard of in San Diego. . .

Appendix 2

Staff ICT Acceptable Use Agreement

I understand that working in an educational context brings with it high expectations of behaviour and integrity, and responsibilities with regard to safeguarding. These expectations include:

- Interacting with pupils in an appropriate way.
- Interacting with colleagues, parents, and other school or work contacts in an appropriate way.
- Being trustworthy with confidential and sensitive information.
- Looking after the fabric and equipment of the school and the GDST, and respecting school property.
- Maintaining the reputation of the school and the GDST (even when not at work).
- Maintaining professional standards of conduct.

These things are equally true when ICT systems, including computers and phones, are involved.

Staff may use school/GDST equipment/network for:

- School/work purposes.
- Reasonable personal use that does not interfere with work.

I understand:

- This agreement applies to the use of GDST ICT systems regardless of location.
- There is a presumption that emails, voice messages and data are stored on GDST equipment for business purposes. This information will be filtered and monitored, and may be accessed to meet business needs.

I will not:

- Do anything that may compromise the safety of children or staff.
- Disclose my username or password to anyone else.
- Try to use any other person's username and password for any purpose.
- Do anything offensive that might bring the school or the GDST into disrepute.
- Access, copy, remove or alter any other user's files without their explicit permission.
- Engage in any on-line activity that may compromise my professional responsibilities.
- Attempt to install programmes on a machine, or store programs on equipment unless approved by school or GDST management.
- Try to circumvent security settings or content filters.
- Deliberately breach anyone's copyright.

I will:

- Bring to the attention of the ICT Department or a member of the Senior Leadership Team any ICT activity or material that may be inappropriate or harmful.
- Report any damage or faults involving equipment or software, however this may have happened, as soon as reasonably possible.
- Only use chat and social networking sites in accordance with the school's and GDST's policies.
- As far as is possible, use GDST email, work phones, and other school communication systems to communicate with pupils. I will only use personal phones or email where the use of GDST systems would be impractical, and I will never communicate with pupils using my personal social media accounts. At all times, I will observe the guidelines on acceptable behaviour contained in the GDST's safeguarding procedures in order to avoid comment or speculation.
- As far as is possible, use GDST provided systems to communicate with parents on school and pupil matters. I will maintain professional standards of conduct if I communicate with parents socially using personal phones, email or social media.

Information Security

I understand that I may have access to sensitive information about colleagues, families or pupils in our care. I will comply with the GDST guidance on data protection and will keep sensitive information within the GDST network. I will not send sensitive information via personal email accounts (Hotmail, GMail etc) or store it on:

- Un-encrypted USB sticks
- Personal devices (phones, laptops) or

- Personal 'Cloud storage' (Dropbox, iCloud)

Images & Videos

In order to prevent allegations of inappropriate activities, including against EYFS staff, I will not store images of pupils on my personal devices. Any images taken on personal devices will be downloaded to school or GDST systems as soon as reasonably possible and the personal copy permanently removed.

Bringing Your Own Device

When I use personal devices in work, I understand that the same expectations of behaviour apply as if I were using school equipment.

I understand that if I fail to comply with this Acceptable Use Agreement, I may have my ICT access suspended and/or be subject to disciplinary action. A copy of this agreement is available upon request and is available within Oracle. I understand a copy of this signed document will be placed on my personal file. I have read and understand the above.

Staff / Volunteer Name	
Signed	
Date	

Reviewed September 2016