ICT Policy

REVIEWED SPRING 2020

‘Green Lane – a Big School with a Big Heart’

This Policy contains the following:

Policy for e-Safety

Staff Acceptable Use of ICT Policy

Pupils Acceptable Use of ICT Policy

Rules for Acceptable Internet Use

Social Media Policy

Policy for e-Safety

This policy should be read in conjunction with other policies including Anti-Bullying, Behaviour, ICT Acceptable Use Policy for Pupils, Safeguarding, Social Media Policy, Staff Acceptable Use of ICT Policy and PSHE.

Throughout the policy, 'Computing' is used to refer to the specific curriculum subject and 'ICT' to describe the broader use of technology.

Introduction
ICT equipment and resources within our academy are provided to enhance pupils' learning and to aid staff in their delivery of the curriculum. These guidelines have been written to ensure that everyone in the academy is aware of what is expected of them and can stay safe when using this hardware and software. This policy sets out a framework for how computing as a subject will be taught in academy and how general use of ICT will be monitored.

Aims
We believe that it is important for children, staff and the wider academy community to have the confidence and ability to use ICT tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent, independent and safe users and learners of Computing we aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use ICT to help improve standards in all subjects across the curriculum
- To develop the ICT competence and skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of academy life
- To use ICT as a form of communication with parents, pupils and the wider community

Curriculum
Computing will be taught across the curriculum and wherever possible, integrated into other subjects, applying skills that have been learnt in computing sessions in cross-curricular

lessons. Our computing curriculum document shows the learning journey which the children are expected to take and this will be maintained to ensure that it is relevant and up-to-date. The New Technologies TLR will work with teachers to ensure that the curriculum provides a broad and progressive development of skills using appropriate software.

Assessment
Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. Children will store their work on the network or in their online Google Sites portfolio which enables staff to view a child's complete portfolio and make summative judgements.

Equal Opportunities and Inclusion
We will ensure that all pupils are provided with opportunities to access the computing curriculum throughout the academy. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve. Children without internet access at home are able to use the academy computers to do any online homework.

Roles and Responsibilities - The Academy
As a academy we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and ICT can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents events.

Roles and Responsibilities - New Technologies TLR
The New Technologies TLR will oversee planning in all year groups throughout the academy and be responsible for raising standards in ICT. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The New Technologies TLR is responsible for overseeing the assessment of ICT across the academy and providing opportunities to moderate ICT ability. They are also responsible for managing equipment and providing guidance for future purchasing.

Roles and Responsibilities - Teachers
Class teachers are responsible for planning, teaching and recording pupil progress in computing in accordance with guidance provided by the New Technologies TLR. Teachers are also responsible for using ICT on an everyday basis with their class, including the use of the touchscreens and interactive whiteboards to provide visual stimulus for learning and providing opportunities to use audio visual equipment such as camera, as well as computing hardware such as iPads and Chromebooks. Teachers should respond to and report any e-safety or cyberbullying issues that they encounter within or out of academy in accordance to e-safety procedures in the Acceptable Usage Policy. Staff should sign and adhere to the Staff AUP.

Roles and Responsibilities - Pupils
Pupils should follow the guidelines laid out in the ICT Acceptable Use Policy for Pupils. They should ensure that they use the computers and equipment appropriately at all times. It is expected that children will follow the academy's Behaviour Policy when working online. They are also expected to adhere to the academy's Anti-Bullying Policy. If the children fail to do so, then the procedures outlined in these policies will be applied.

Roles and Responsibilities - Parents
Parents are asked to sign the Internet Use Agreement and to discuss this with their child. Parents should stay vigilant to the websites and content that their children are accessing and try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the New Technologies TLR or the Head Teacher.

Roles and Responsibilities - Governors and Visitors
Academy governors should abide by the guidelines set out for staff and ensure that any use of computers and equipment within academy is carried out in accordance with this. If either a visitor or governor wishes to have a temporary account to logon to the academy network, they should speak to the New Technologies TLR.

Equipment - Hardware and Software
ICT equipment should be used with care to preserve life and prevent wastage. To promote this, no food and drink is allowed near equipment in the classroom. Communal resources such as iPads and Chromebooks should be returned after use to ensure availability for other classes. Student iPads should not be kept by teachers – they should be returned to the storage trolleys after use. Any work that needs to be taken off a device should be done so quickly, using Staff or Pupil Google Drives as a storage location, and the device returned to the storage trolleys. Hardware should not be installed without the permission of the New Technologies TLR. The installation of software unauthorised by the academy, whether licensed or not, is forbidden. If you are unsure, please speak to the New Technologies TLR for advice. The academy reserves the right to examine or delete any files that are held on its system.

Sustainability and Environmental Impact
Hardware is disposed of safely and securely in accordance with WEEE.

Network
Accounts on the network are created and monitored by the academy's appointed ICT provider, Activ Technology. Staff are issued with a username for the network and a temporary password which needs to be changed in accordance with the password procedure below. Children have individual logins based on their full name as given in SIMS except where variations are requested by class teachers prior to the creation of logins. There is a uniform password for children. Children are also given a Google email address and password that enables them to log on to the Chromebooks and access their cloud storage. The creation of these is managed by Activ Technology, and any requests for new users need to go through the New Technologies TLR.
When a new child joins, it is the responsibility of the class teacher to inform the New Technologies TLR of the child's name and year group either via email or the ICT Log Book in the Staff Room. The ICT provider will then provide a network login and accounts for online tools. At the end of a child's time with us, they will be able to take their academywork with them if requested. Once they have left our academy, the child's account and their content will be removed.
The academy has a wireless network for use with academy hardware. There is also a Guest network which can be used by visitors and staff to connect phones and laptops when necessary. On request, the IT Coordinator will enter the Wi-Fi password.

Passwords
Activ Technology holds the passwords to different areas of the academy network and has administrator access. Users will be given access to systems at the appropriate level.
All staff have password protected access to the academy network and the initial password must be changed at first login. Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. Staff are prompted to change their password every three months. Staff should be aware of and apply the guidance given in the Staff AUP with regard to data security.
For online services used in academy such as Target Tracker, there is academy password which allows staff to access the programme. It is important that these details are not accessible to pupils at any point.
For sites such as Times Table Rockstars, children have personal passwords. These passwords are site-specific and as children progress through the academy they will be taught about choosing sensible and secure passwords for online sites and apps.

Backups
The data stored on the academy's network is backed up on site and remotely by Activ Technology. Staff need to notify the New Technologies TLR immediately if they realise something has been accidently deleted so that copies of files can be recovered.

Technical Support
A detailed description of any equipment failure or error should be recorded by staff in the ICT log book in the Staff Room. Minor issues will be dealt with by the New Technologies TLR as appropriate. Hardware and software technical support is provided remotely and on-site by Active Technology when required. Staff should email the helpdesk at it@helloactiv.co.uk.

Academy Website
The academy website is updated by the Digital Profile TLR. All classes can submit documents and photographs for publication. Photographs including images of children need to be checked for parental permission and meet the criteria shown below before submission.

Digital and Video Images
As an academy we will ensure that if we publish any photographs or videos of children online, we will:
• ensure that their parents or guardians have given us written permission.
• ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily.
• not include a child's image and their full name together without permission from the parents or guardians e.g. if the child has won an award.
• ensure that children are in appropriate dress.
• remove photos at the request of a parent or guardian. This request can be made in writing to the child's teacher or to the New Technologies TLR. We will endeavour to remove the photograph as soon as possible.
• ask parents or guardians who are recording video or taking digital images at public events e.g. academy play or sports day, that they do not publish these online.

Prevent Duty
Academies are expected to ensure children are safe from terrorist and extremist material when accessing the internet in academy. This is achieved at Green Lane Primary Academy by establishing appropriate levels of filtering.

Internet and E-mail
The internet may be accessed by staff and by children throughout their hours in academy and users are responsible for ensuring that they have logged off so that other users cannot access previously accessed sites. Staff need to be vigilant as to the sites children are accessing and children should not be using the internet unattended. The teaching of email, internet use and other aspects of e-safety will be covered within the computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet. If users, especially children, see an inappropriate website or image, they should minimise the page immediately and report the site to their class teacher who will report this to the New Technologies TLR. Active Technology will be contacted to attempt to get this site blocked.
Children are issued with an individual academy email address in order to access the G Suite tools, but this is limited to contact within academy only. They are unable to use it to contact external addresses. Staff are provided with an academy Office 365 email address and need to follow the guidelines in the Staff AUP when using this.

Social Media
As an academy we recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should apply the guidance given in the Staff AUP and Social Media policies with regard to social networking.
Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a academy, we reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyberbullying, occur.

E-Safety
We take e-safety seriously and will ensure that computing and PSHE sessions teach how to minimise the risk when working on the internet, managing passwords and respecting copyright, as relevant to the children's age. All children will be taught about the Internet Acceptable Use Policy and will sign a copy. Useful ICT rules will also be displayed to ensure they are seen by children and visitors.
If a teacher suspects an E-safety issue within academy they should make notes related to the incident in accordance with academy Anti-bullying and Behaviour policies. This should then be reported to the New Technologies TLR and Headteacher; recorded and parents contacted as appropriate.

Cyberbullying
Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites.

Through Computing lessons, assemblies and PSHE, children will be taught the **SMART** rules:

Safe	Keep safe by being careful not to give out personal information online.
Meeting	Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.
Acceptable	Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.
Reliable	Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.
Tell	If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place Or call a helpline like ChildLine on 0800 1111 in confidence.

Copyright
Copyright of materials should be respected. Staff should check permission rights before downloading material, particularly images from the internet, and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it. Children will be taught that it is not acceptable to take images directly from the internet without permission for use and to start referencing the sites they have used.

Responding to unacceptable use by pupils
Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the Behaviour and Anti-bullying policies as necessary.

Responding to unacceptable use by staff
Failure to comply with the guidelines and expectations in the Staff AUP could lead to sanctions and possible disciplinary action in accordance with the academy's policies and the law.

Acceptable Use Policy - Governors and Visitors
Visitors may be provided with accounts to our network and/or online systems on a case-by-case basis, depending on the purpose of the account requested. Users will be expected to follow the guidelines as set out for staff and understand that accounts may be removed at any time.

Complaints
Incidents regarding the misuse of the Internet by students will be forwarded to the Headteacher and New Technologies TLR who will decide whether additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the Headteacher. Complaints of a safeguarding nature must be dealt with in accordance with safeguarding procedures.

Staff ICT Acceptable Use Policy

Introduction
This policy should be read in conjunction with other relevant academy policies, procedures and codes of conduct including:
• Social Media Policy
• ICT Policy
• Disciplinary Procedure

This policy applies to the academy governing body, all teaching and other staff, external contractors providing services on behalf of the academy, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the academy. These individuals are collectively referred to in this policy as staff or staff members.

Staff should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role.

It is not the intention of the policy to try to police every social relationship that teachers may have with parents and governors but about reminding individuals of the importance of appropriate boundaries, including through their social media use.

Application

The policy applies in respect of all ICT resources and equipment within the academy and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of academy internet access and email systems, software (including use of software such as SIMS), academy telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work. This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

Access
Academy staff will be provided with a log on where they are entitled to use the academy ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the academy to benefit from such facilities.

Where staff have been provided with an academy email address to enable them to perform their role effectively, it will not normally be used to communicate with parents and pupils. Where staff are able to access email outside of academy's hours, the email facility should not routinely be used to email parents outside of normal academy hours. Accessing emails

via a phone or tablet must be done through the Microsoft Outlook app, and staff must not use third-party email applications to access their work emails.

Access to certain software packages (SIMS, CPOMS, Target Tracker, remote access) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their academy laptop/other equipment is password protected and not accessible by others. When in use at home it must not be used inappropriately by themselves or others. Staff must also ensure that they bring their laptop into school as required for updating of software, licences and virus protection.

Where the academy provides digital cameras, iPads and other recording equipment for educational and academy business use, and it is used away from the academy site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the academy's policy in relation to use of pictures, is followed.

Staff may use, in urgent or emergency situations during off site visits, their personal mobile phones. Should staff need to make contact whilst off site, this should normally be undertaken via the academy rather than a direct call from the individual's personal mobile. Academy staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

Communication with Parents, Pupils and Governors
The academy communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content.

Academy Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/academy link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Head Teacher before sending. Where office staff send letters home these will normally require approval by the Head Teacher.

Email – academy email accounts should not routinely be used for communication with parents outside academy hours.

Under normal circumstances, academy staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Head Teacher.

4.3 Where pupils are submitting work electronically to academy staff, this must be undertaken using academy systems such as Google Classroom and not via personal email.

Social Media
Academy staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the academy can lead to disciplinary action, including dismissal.

Staff should refer to the Academy Social Media AUP which contains detailed advice on the expectations of staff when using social media.

Unacceptable Use
Appendix 1 provides a list of Do's and Don'ts for academy staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. Academy systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the academy or to communicate/share confidential information which the member of staff does not have authority to share

- to present any personal views and opinions as the views of the academy, or to make any comments that are libellous, slanderous, false or misrepresent others

- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material

- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally

- to communicate anything via ICT resources and systems or post that may be regarded as critical of the academy, the leadership of the academy, the academy's staff or its pupils

- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment

- to collect or store personal information about others without direct reference to The Data Protection Act

- to use the academy's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project

- to use the academy computers to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the academy

- to undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for the safeguarding of children and young people.

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or New Technologies TLR if applicable.

Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Head Teacher or other member of the senior leadership team, as well as the New Technologies TLR. The academy does use appropriate blocking software to avoid the potential for this to happen. Reporting to the Head Teacher, senior leadership team or New Technologies TLR equally applies where academy staff are using academy equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Head Teacher or another member of the senior leadership team so that this can be dealt with appropriately.

Personal and Private Use

All academy staff with access to personal computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the academy
- detrimental to the education or welfare of pupils at the academy

Excessive personal use of academy facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the academy will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

Where academy staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the academy, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time.

Whilst individuals may be required to use their personal mobile telephone to make contact with the academy, staff should exercise care as outlined in section 3.

Security and Confidentiality
Any concerns about the security of the ICT system should be raised with the New Technologies TLR

Staff are required to ensure that they keep any passwords confidential, select a password that conforms to the requirements of the e-safety policy and change passwords when prompted to by the system.

Academy staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the academy server. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the academy's systems. Where problems are encountered in downloading material, this should be reported to the academy's ICT lead.

Where staff are permitted to work on material at home, staff should normally use their academy issued laptop for such work. Remote access to the server has been set-up to allow this. Any work done on personal computers should be uploaded to staff member's Google Drive to be accessed in academy, or uploaded to the academy network via remote access. Use of memory sticks is not permitted.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or Google Drive.

Whilst any members of academy staff may be involved in drafting material for the academy website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

Activ Technology are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all academy based and academy issued equipment. Staff must ensure that they notify Activ when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the academy's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, using encrypted laptops. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with. Where appropriate, staff should either password protect sensitive files, or send via encrypted emails.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Monitoring
The academy reserves the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the academy's hardware, software, networks and systems are not compromised

- to prevent or detect crime or unauthorised use of the academy's hardware, software, networks or systems

- to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the academy may track the history of the internet sites that have been visited.

Whistleblowing and Cyberbullying
Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Head Teacher to such abuse in accordance with the academy's Whistleblowing policy. Where a concern relates to the Head Teacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of academy staff. Staff should follow the advice within the Harassment, Discrimination and Bullying Policy for School Staff if they feel concerned. Advice can also be sought from professional associations and trade unions. Support is also available through the UK Safer Internet Centre helpline@safetinternet.org.uk or 0844 381 4772

Signature
It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

Do's and Don'ts: Advice for Staff **Appendix 1**

Whilst the wide range of ICT systems and resources available to staff, both in academy and outside of academy, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of academy.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues:

Do

- ensure that you do not breach any restrictions that there may be on your use of academy resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the academy's ICT resources and facilities
- be aware that the academy's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the academy's systems, resources and equipment to the Headteacher or New Technologies TLR and/or Designated Safeguarding Lead (DSL) as appropriate
- be aware that a breach of your academy's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access academy systems and resources
- download, upload or install any hardware or software without approval
- use removable storage devices to store personal data
- use academy systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of telephones, mobile telephones and instant messaging:

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your academy's policy on use of personal mobile telephones

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the academy's telephone system for personal calls
- use personal or academy mobile telephones when driving

• use the camera function on personal or academy mobile telephones to take images of colleagues, pupils or of the academy

Use of cameras and recording equipment:

Do	Don't
• ensure that material recorded is for educational purposes only • ensure that where recording equipment is to be used, approval has been given to do so • ensure that material recorded is stored appropriately and destroyed in accordance with the academy's policy • ensure that parental consent has been given before you take pictures of academy pupils	• inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded

Use of email, the internet, Google Drive and academy network:

Do	Don't
• alert your Head Teacher or designated manager if you receive inappropriate content via email • be aware that the academy's email system will be monitored and recorded to ensure policy compliance • ensure that your email communications are compatible with your professional role • give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate • be aware that the academy may intercept emails where it believes that there is inappropriate use • seek support to block spam • alert your Head Teacher or designated manager if you accidentally access a website with inappropriate content • be aware that a website log is recorded by the academy and will be monitored to ensure policy compliance • answer email messages from pupils and parents within your directed time	• send via email or download from email, any inappropriate content • send messages that could be misinterpreted or misunderstood • use personal email addresses to communicate with pupils or parents • send messages in the heat of the moment • send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude • use email systems to communicate with parents or pupils unless approved to do so • download attachments from emails without being sure of the security and content of the attachment • forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention • access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the academy network or Google Drive • upload any material onto the academy website that doesn't meet style requirements and without approval

Cyber-bullying: Practical Advice for Academy Staff

The development of new technologies and systems e.g. mobile phones, email and social networking websites means that bullying is often now taking on a new form; cyber-bullying. Victims of cyber-bullying can experience pain and anxiety as much as traditional forms of bullying, particularly as it can occur outside of the academy and academy hours, significantly intruding into the personal life of the victim. Whilst it is difficult for academies and teachers to deal with this as they have no direct control over external websites there are a range of actions that academy staff can take to reduce the chances of cyber-bullying occurring and actions that can be undertaken where it has already occurred.

The guidelines for Headteachers and Governors in dealing with allegations of bullying or harassment define cyberbullying as "the use of information and communication technologies to threaten, harass, humiliate, defame or impersonate". Cyberbullying may involve email, virtual learning environments, chat room, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites.

This practical advice supplements the guidelines and provides links to other guidance available to academy staff in relation to Cyberbullying.

DOs

• Keep passwords confidential

• Ensure you familiarise yourself with your academy's policy for acceptable use of technology, the internet, email and HCC and academy intranets.

• Ensure any social site you use has restricted access

• Ensure that you understand how any site you use operates and therefore the risks associated with using the site

• Consider carefully who you accept as friends on a social networking site

• Report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site

• Check what images and information is held about you online but undertaking periodic searches of social networking sites and using internet search engines

• Take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain

• Be aware that any off-duty inappropriate conduct, including publication of inappropriate images and material and inappropriate use of technology could lead to disciplinary action within your employment

• Liaise with your Headteacher and Head/Leader of ICT to remove inappropriate material if it appears on the academy website

• Take screen prints and retain text messages, emails or voice mail messages as evidence

• Follow academy policies and procedures for e-safety, including access to and use of email, internet and HCC intranet

• Follow academy procedures for contacting parents and/or pupils

• Only contact pupils and/or parents via academy based computer systems

• Keep your mobile phone secure at all times

• Answer your mobile telephone with 'Hello' rather than your name, if the number on the display is unknown to you

• Use a academy mobile phone where contact with parents and/or pupils has to be made via a mobile (eg during an educational visit off site)

• Erase any parent or pupil data that is stored on a academy mobile phone after use

• Seek support from your manager, professional association/trade union, friend, employee support line as necessary

• Report all incidents of cyberbullying arising out of your employment to your Headteacher

• Report any specific incident on a Violent Incident Report (VIR) form as appropriate

• Provide a copy of the evidence with your Headteacher when you report it and further evidence if further incidents arise
• Seek to have offensive online material removed through contact with the site
• Report any threatening or intimidating behaviour to the police for them to investigate
• Access and use the DCSF guidance on Cyberbullying, specifically the advice on reporting abuse and removal of material/blocking the bully's number/email (see attachment/link below)
• Support colleagues who are subject to cyberbullying

DON'Ts

• Allow any cyberbullying to continue by ignoring it and hoping it will go away
• Seek to return emails, telephone calls or messages or retaliate personally to the bullying
• Put information or images on-line, take information into academy, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial
• Accept friendship requests from pupils or parents
• Release your private e-mail address, private phone number or social networking site details to pupils and parents
• Use your mobile phone or personal e-mail address to contact parents and/or pupils
• Release electronically any personal information about pupils except when reporting to parents
• Pretend to be someone else when using electronic communication
• Take pictures of pupils with academy equipment without getting parental permission or without being directed to undertake such activity for an appropriate specified purpose
• Take pictures of pupils on your own equipment

Childnet International have produced a document, "Cyberbullying: Supporting Academy Staff" which is a useful source of reference to all academy staff and leaders. This is available at http://www.childnet.com/ufiles/cyberbullying_teachers.pdf
Further guidance is available to academys in relation to Cyberbullying as a whole academy community and specifically in relation to cyberbullying of and by pupils via:
• www.teachernet.gov.uk
• www.becta.org.uk
• www.digizen.org

Staff Code of Conduct for ICT **Appendix 2**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the academy's Policy for Staff Acceptable Use of ICT for further information and clarification.

• I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and network access and use of social networking and that ICT use may also include personal ICT devices when used for academy business
• I understand that it may be a criminal offence to use the academy ICT system for a purpose not permitted
• I understand that I am unable to communicate information which is confidential to the academy or which I do not have the authority to share
• I understand that academy information systems and hardware may not be used for personal or private use.
• I understand that my use of academy information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
• I understand the level of authority required to communicate with parents and pupils using the various methods of communication
• I understand that I must not use the academy ICT system to access inappropriate content
• I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
• I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
• I will not install any software or hardware without permission
• I will follow the academy's policy in respect of downloading and uploading of information and material
• I will ensure that personal data is stored securely and is used appropriately whether in academy, taken off the academy premises or accessed remotely. I will not keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
• I will respect copyright, intellectual property and data protection rights
• I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
• I will report any incidences of concern regarding children's safety to the Safeguarding and Pastoral Lead or Head Teacher.
• I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Head Teacher, or if appropriate, the Chair of Governors
• I will ensure that any electronic communication undertaken on behalf of the academy, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
• I understand the academy's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
• I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
• I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
• I understand that inappropriate use of personal and other non-academy based ICT facilities can have implications for my employment at the academy where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children.

The academy may exercise its right to monitor the use of the academy's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the academy's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from the New Technologies TLR.

SIGNED: …… DATE: ……

NAME (PRINT): ……

Pupils Acceptable Use of ICT Policy

This policy outlines our purpose in providing access to the Internet, e-mail and other communication technologies at Green Lane Primary Academy and explains how the academy is seeking to avoid the potential problems that unrestricted access could create.

Internet Access in Academy

• All staff and any other adults involved in supervising children accessing the Internet, will be provided with the academy ICT Acceptable Use Policy, and will have its importance explained to them.

• Our academy ICT Acceptable Use Policy for Pupils is available for parents on the academy website.

Using the Internet to Enhance Learning

Access to the Internet is a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

• access to the Internet may be by teacher demonstration

• pupils may be given a suitable web site to access using a link from their year group links page on the academy website or by clicking on a link in a teacher-prepared Word document

• pupils may be provided with lists of relevant and suitable web sites which they may access

• older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected act responsibly and will be informed that checks can and will be made on files and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times. Discussions will be had with pupils around appropriate internet behaviour. Teachers will endeavour to ensure that these expectations remain uppermost in the children's minds as they monitor the children using the Internet.

Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it:

• pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the academy library or on television

• teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium)

• when copying materials from the Web, pupils will be taught to observe copyright;

• pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using E-mail

It is important that communications are properly managed to ensure appropriate educational use and that the good name of the academy is maintained. Therefore:

• incoming and outgoing e-mail is accessed via Gmail and not downloaded onto academy computers

• pupils may send e-mail as part of planned lessons but this will only be to other greenlanemiddlesbrough.co.uk addresses.

• pupils will only be allowed to use class email once they have been taught how to use the tool responsibly

• teachers will endeavour to ensure that these responsibilities remain uppermost in the children's minds as they monitor children using e-mail

• incoming e-mail to class e-mail addresses will not be regarded as private

• pupils will not be permitted to use e-mail at academy to arrange to meet someone outside academy hours

• the forwarding of chain letters will not be permitted.

Ensuring Internet Access is Appropriate and Safe

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in academy are unlikely to see inappropriate content in books due to selection by publisher and teacher and the academy will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

• our Internet access includes a filtering system intended to prevent access to material inappropriate for children;

• children using the Internet will normally be working during lesson time and will be supervised by an adult (usually the class teacher) at all times;

• staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;

• staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

• pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others;

• the ICT co-ordinator will monitor the effectiveness of Internet access strategies;

Generally, the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. The academy will not accept liability for the material accessed, or any consequences of this.

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, responsibility for handling incidents involving children will be taken by the New Technologies TLR and the Safeguarding and Pastoral Lead in consultation with the Head

Teacher and the pupil's class teacher. All the teaching staff will be made aware of the incident if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the academy has taken. The academy aims to work with parents/carers and pupils to resolve any issue.

- If staff or pupils discover unsuitable sites the New Technologies TLR will be informed. The New Technologies TLR will report the URL and content to the ISP; if it is thought that the material is illegal, after consultation with the ISP, the site will be referred to the Internet Watch Foundation http://www.iwf.org.uk and the police.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use that have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when undertaking their own Internet search, then sanctions consistent with our Academy Behaviour Policy will be applied. This will involve informing the parents/carers. Access to the Internet may also be denied for a period.

Photographs
Prior permission is sought from all parents regarding the use of images for printed publications, media, website and videos. Staff should check the relevant year group permission list before using images of children.

Cyberbullying
Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites.
Through Computing lessons, assemblies and PSHE, children will be taught the **SMART** rules:

Safe	Keep safe by being careful not to give out personal information online.
Meeting	Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.
Acceptable	Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.
Reliable	Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.
Tell	If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place Or call a helpline like ChildLine on 0800 1111 in confidence.

GREEN LANE PRIMARY ACADEMY

Rules for Responsible Internet Use

The academy has computers with Internet access to help you with your learning. These rules need to be signed before you use the Internet and will help you to keep safe and be fair to others.

Using the Computers:

• I will only access the academy network with the login I have been given.
• I will not try to access files in other people's folders.
• I will close all programs and log out before leaving the computer.
• I will ensure that any DVDs/USB drives that I bring in from outside academy have been virus-checked before using them on the academy computers.

Using the Internet:

• I will ask permission from a teacher before using the Internet.
• I will only search the Internet in ways that my teacher has approved.
• I will check who owns an image I may want to use on the Internet and will only use those with permission for re-use.
• I will minimise the web page if I find any unpleasant material and will report this to my teacher immediately because this will help protect other pupils and myself.
• I understand that the academy may check my computer files, and may monitor the Internet sites I visit.

Using e-mail / messaging / forms:

• I will not give my full name, date of birth, home address or telephone number on any website.
• I will not share anyone else's personal information online.
• I will not use the Internet to arrange to meet someone outside academy hours.
•I will ask permission from a teacher before sending any messages on the Internet and will only send messages to people / sites that my teacher has approved
• The messages I send will be polite and responsible.
• I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.

Signed …… **(Child)**

…… **(Parent)**

Date ……

Social Media Policy

Introduction to the Policy

The academy is aware and acknowledges that increasing numbers of adults and children are using social networking sites. Some with the widest use are Instagram, Facebook and Twitter.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance is to protect staff and advise academy leadership on how to deal with potential inappropriate use of social networking sites.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

Purpose

The purpose of this policy is to ensure:

• That the academy is not exposed to legal risks

• That the reputation of the academy is not adversely affected

• That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the academy.

Facebook is targeted at older teenagers and adults. They have a no under-13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy:

"*If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us*"

Scope

This policy covers the use of social networking applications by all academy stakeholders, including, employees, governors and pupils. These groups are referred to collectively as 'academy representatives' for brevity.

The requirements of this policy apply to all uses of social networking applications which are used for any academy related purpose and regardless of whether the Academy representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:

Blogs, for example Blogger

Online discussion forums, such as netmums.com

Collaborative spaces, such as Facebook

Media sharing services, for example YouTube

'Micro-blogging' applications, for example Twitter

All academy representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Use of Social Networking Sites in Worktime
Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Head teacher.

Social Networking as Part of Academy Service
All proposals for using social networking applications as part of an academy service (whether they are hosted by the academy or by a third party) must be approved by the Head Teacher first.

Use of social networking applications which are not related to any academy services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head teacher. However, academy representatives must still operate in line with the requirements set out within the policy.

Academy representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all academy representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on academy network or not.
Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

Green Lane Primary Academy expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Terms of Use
Social Networking applications:
• Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the academy into disrepute.
• Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
• Must not be used in an abusive or hateful manner
• Must not be used for actions that would put academy representatives in breach of academy codes of conduct or policies relating to staff.

• Must not breach the academy's misconduct, equal opportunities or bullying and harassment policies

• Must not be used to discuss or advise any matters relating to academy matters, staff, pupils or parents

• No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with

• Employees should not identify themselves as a representative of the academy

• References should not be made to any staff member, pupil, parent or academy activity / event unless prior permission has been obtained and agreed with the Head Teacher

• Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/Protection for Staff on Using Social Networking

• No member of staff should interact with any pupil in the academy on social networking sites

• No member of staff should interact with any ex-pupil of the academy on social networking sites who is under the age of 18

• This means that no member of the academy staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.

• Where family and friends have pupils in academy and there are legitimate family links, please inform the Head Teacher in writing. However, it would not be appropriate to network during the working day on academy equipment.

• It is illegal for an adult to network, giving their age and status as a child

• If you have any evidence of pupils or adults using social networking sites in the working day, please follow the guidance detailed within the academy's Whistleblowing Policy

Guidance/Protection for Pupils on Using Social Networking

• No pupil under 13 should be accessing social networking sites. This is the guidance from Facebook. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is: http://www.facebook.com/help/contact.php?show_form=underage

• No pupil may access social networking sites during the academy working day

• Year 6 pupils who are walking to and from academy by themselves are permitted to bring a mobile phone to academy. These mobile phones must be switched off on academy property and handed into the office at the beginning of the academy day.

• No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens

• No academy computers are to be used to access social networking sites at any time of day unless for direct academy use (posting academy information of the academy Facebook page.)

Any attempts to breach firewalls will result in a ban from using academy ICT equipment other than with close supervision

• Please report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.

• We have a zero tolerance to cyber bullying

Child Protection Guidance
If the Head Teacher receives a disclosure that an adult employed by the academy is using a social networking site in an inappropriate manner as detailed above they should:
• Record the disclosure in line with the Child Protection Policy
• If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
• If disclosure comes from a member of staff, try to maintain confidentiality

• The LADO will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
• If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out.

Cyber Bullying
By adopting the recommended no use of social networking sites on academy premises, Green Lane Primary Academy protects themselves from accusations of complicity in any cyber bullying through the provision of access.
Parents should be clearly aware of the academy's policy of access to social networking sites. Where a disclosure of bullying is made, the academy now has the duty to investigate and protect, even where the bullying originates outside the academy.

This can be a complex area, and these examples might help:

• A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not an academy responsibility, though the academy might contact the new academy to broker a resolution.
• A child is receiving taunts from peers. It is all at weekends using Facebook or texts. The pupils are in the academy.The academy has a duty of care to investigate and work with the families, as they attend the academy.
• A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5. The academy has a duty of care to investigate and work with the families, as they attend the academy. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the academy, the academy could legitimately say that the victims and perpetrators had failed to follow the academy's recommendation. They could then deal with residual bullying in the academy, but refuse to deal with the social networking issues.

• Once disclosure is made, investigation must involve the families. This should be dealt with under the academy's anti-bullying policy.

• If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment

• This guidance can also apply to text and mobile phone cyber bullying.

• If a parent/carer is making threats on-line against a member of academy staff – this is counted as bullying. The member of staff must inform the Head teacher immediately and the parent/carer spoken to. Should the situation not be resolved, the police and LA should be informed.