E-Safety, Social Networking & Acceptable Use of ICT Policy 2020- 2022

Chair of Governors signature	
Headteacher signature	
Policy type (statutory / non-statutory)	
Date	Approved by FGB: 03/02/21
Next review date	

To inspire and educate for life

E- Safety, Social Networking and Acceptable Use of ICT Policy

The policy has been developed having regard to guidance provided by the professional associations for teachers and school leaders, other recognised trade unions, and by ACAS. It sets out the rules and standards to be applied for use of the Internet and social media in Hampshire schools. It provides information and guidance for both professional and personal use and outlines the risks to users and schools, as well as the potential consequences of misuse of the Internet and social media.

Schools are encouraged to ensure that staff are 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. Schools and their staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com).

Where staff have concerns about e-safety, these should be raised with the Headteacher. Advice can also be sought from professional associations and trade unions.

This Policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- Disciplinary Procedure
- Remote Learning Plan
- Home Learning E-Safety Policy

Contents

1. Introduction and Application

a. This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as 'staff' or 'staff members'.

   The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school 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.

It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media for new opportunities for communication, this policy sets out the principles that school staff, governors and contractors are required to follow when using social media.

It is essential that pupils/students, parents and the public at large have confidence in the school’s decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the school who use the Internet and social networking sites. It is also aimed at ensuring that the Internet and social media are utilised safely, lawfully and effectively for the successful and economic delivery of school-based services.

b. Responsibilities of Staff Members

The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of the School.

The School has a duty to provide a safe working environment free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the School, or people receiving services from the School then any information posted must comply with all relevant professional Codes of Practice.

This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the school’s reputation, school information or computer systems/networks.

c. Access

School staff will be provided with a log on where they are entitled to use the school 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 school to benefit from such facilities.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless the admin office, or a member of SLT, is also copied into the conversation. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), CPOMs, SIMS, RAISE Online, FFT, school texting services) 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 school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school 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 school's policy in relation to use of pictures, is followed.

If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

2. Risks involved with ICT at schools:

The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its pupils, its staff and the people it serves. Principal amongst these risks are:

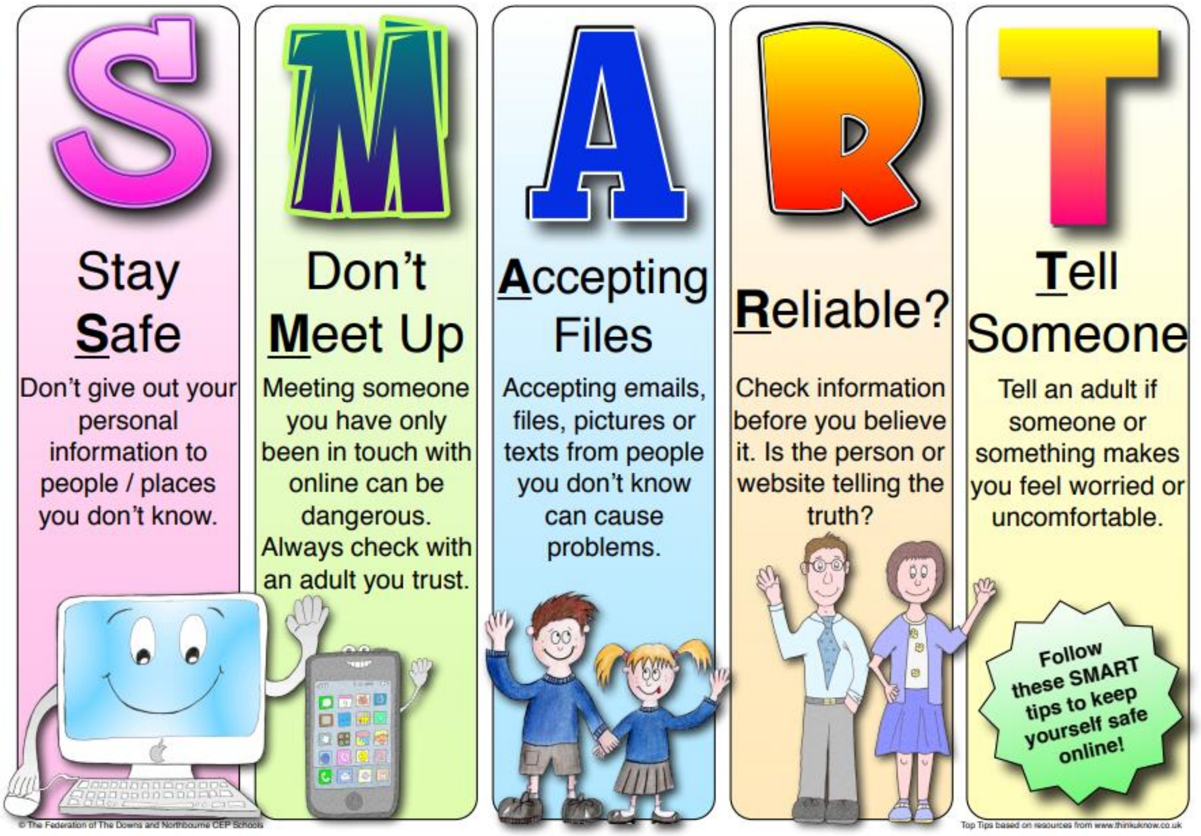
- cyber bullying by pupils/students (see section 9 for more detail);
- access to inappropriate material;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the school;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

3. Risk mitigation for Pupils

a. E-safety in the Curriculum

Teaching children about e-safety is a key part of the Computing Curriculum. E-safety is embedded throughout the curriculum; it will be constantly referred to in lessons when appropriate. On top of this, there are additional e-safety events run throughout the year.

Children are taught to **be 'SMART' online**. See figure 1 below.


S
M
A
R
T
Stay Safe
Don't give out your personal information to people / places you don't know.
Don't Meet Up
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
Accepting Files
Accepting emails, files, pictures or texts from people you don't know can cause problems.
Reliable?
Check information before you believe it. Is the person or website telling the truth?
Tell Someone
Tell an adult if someone or something makes you feel worried or uncomfortable.
Follow these SMART tips to keep yourself safe online!

© The Federation of The Downs and Northbourne CEP Schools

Top Tips based on resources from www.thinkuknow.co.uk

Figure 1: SMART poster: these are on prominent display around the school

Children (and their parents) are also required to sign a 'Code of Conduct for Internet and e-mail use for Pupils/Parents' before they are allowed to access ICT at school – see appendix 4.

b. Ensuring Internet Access is Appropriate and Safe

In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. The school 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 is purchased from Hampshire County Council which provides a service designed for pupils including a “firewall” 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 at all times;
- Staff will be particularly vigilant when pupils are undertaking their own searches;
- Pupils will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others;
- Our ‘SMART’ posters will be posted prominently around the school;
- The IT co-ordinator will monitor the effectiveness of internet access strategies;
- The head teacher will ensure that the policy is implemented effectively;
- Methods to quantify; and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfE.

It is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequences thereof.

A most important element of e-safety is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

c. Using Information from the Internet

We believe that, 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. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it is copyrighted.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;

- 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;
- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the IT Co-ordinator and the DSL in consultation with the Head Teacher and the pupil's class teacher;
- 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 school has taken. The school aims to work with parents/carers and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the IT Co-ordinator will be informed. The IT Co-ordinator may then use the web filtering system to prevent further access.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by staying 'SMART' online. 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 given the privilege of undertaking their own search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to the internet may be denied for a period.

4. Risk mitigation for Staff

a. **Unacceptable Use**

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

- to communicate any information that is confidential to the school 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 school, 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 school, the leadership of the school, the school'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 collect, store or share personal data in accordance to GDPR;
- to use the school'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 visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school – these will most likely be blocked by the web filtering service anyway;
- 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 ICT lead if applicable.

Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the Senior Leadership Team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or Senior Leadership Team equally applies where school staff are using school 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 Headteacher or another member of the Senior Leadership Team so that this can be dealt with appropriately.

b. Using the Internet and Social Media for Approved School Purposes

Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school's reputation and credibility or otherwise violate any school policies. In particular:

- the school’s Internet connection is for business use and its use, and use of social networking, must only take place in line with the school’s policies;
- when acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- personal email or social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- staff members must report any safeguarding issues they become aware of;
- staff members must not cite or reference pupils/students/parents without approval;
- material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- material published must be truthful, objective, legal, decent and honest;
- material published must not breach copyright;
- any publication must comply with all of the requirements of the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with school policies;
- if used with pupils/students, staff must ensure that the site’s rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.

c. Personal Use of Internet and Social Media

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this 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 school
- detrimental to the education or welfare of pupils at the school

The school's Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for personal use and access can be withdrawn at any time. Where staff members are permitted to use the school's Internet connection for personal use:

- the school is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- staff wishing to spend significant time outside of their own normal working hours using the Internet at school – e.g. for study purposes - must obtain prior approval;
- inappropriate or excessive use at school may result in disciplinary action and/or removal of Internet facilities;
- the school will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the school's Internet facility;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only according to the Council's Internet, Intranet and Email Monitoring Policy and School's disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a colleague, or some other legitimate and objective complaint or incident;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff concerned about this should refrain from using the Internet for private matters;
- due to the potential impact on school systems, the downloading of media for **personal** use such as video (YouTube, BBC iPlayer, Vimeo etc.);
- certain websites will be blocked, but it is a breach of this guide to access any of the following types of site:

  - pornography/Adult/mature content
  - gambling/betting/gaming
  - alcohol/Tobacco
  - illegal drugs
  - auction sites
  - violence/hate/racism
  - weapons
  - any site engaging in or encouraging illegal activity
  - illegal file-sharing sites

- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Senior Leadership Team. Genuine mistakes and accidents will not be treated as breach of this policy;
- staff members may not download software from any source without approval;
- staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Headteacher;
- staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorised to do so by their Senior Leadership Team;
- users must not create, download, upload or transmit any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- users must not create, download, upload or transmit any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- users must not create, download, upload or transmit material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others;
- users must not create, download, upload or transmit any unsolicited commercial or bulk web mail, chain letters or advertisements;
- users must not download any digital media including music, images, photos and video that would be in breach of copyright or licensing arrangements, or where copyright or ownership cannot be determined;
- the use of file sharing services or software is prohibited for any purpose;
- the use of cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud, is not permitted for the storage of sensitive personal data.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time (e.g. on their mobile phones at breaktime or at home) 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 school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, 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. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

d. Social Media

School 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 school can lead to disciplinary action, including dismissal.

e. School Reputation and Confidentiality

The school recognises an employee's right to a private life. However the school must also ensure its reputation and confidentiality are protected. Therefore an employee using any ICT away from school, including email and social networking sites must:

- **refrain from identifying themselves as working for the school** in a way that could have the effect of bringing the school into disrepute
- not express a personal view as a school employee that the school would not want to be associated with
- notify the Senior Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school
- **not have any contact or accept 'friend' requests through social media with any pupil/student under the age of 18** (or under age 19 where the school has such provision), (including former pupils/students and/or those who attend other schools) unless they are family members;
- exercise **caution when having contact or accepting 'friend' requests through social media with parents** so as not to compromise the school's reputation or school information;
- not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents
- **not disclose any data or information about the school**, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the General Data Protection Regulations (**GDPR**) 2016 and the Data Protection Act 2018
- not use the Internet or social media in or outside of work to bully or harass other staff or others

- any concerns about the security of the ICT system should be raised with a member of the Senior Leadership Team.
- staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.
- school staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should be used. 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 school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.
- Where staff are permitted to work on material at home and bring it in to upload to the school server through their USB sticks, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.
- 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 VLE.
- Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.
- The school will use the services of Harrap who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.
- Staff must ensure that their use of the school'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, either through password protection on USB sticks or through encrypted USB sticks. 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.
- 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.

5. Managing Emerging Technologies

We are aware that technology is always changing. This provides huge benefits but also creates potential risks. As such, emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Staff will also stay vigilant for any new potential risks that may arise from technology that children use at school or home.

The Senior Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

a. Mobile phones for Pupils and Parents

- Mobile phones will not be used by children during lessons or formal school time. All mobile phones brought to school must be given in to the office at the start of the day, and returned to the child at the end of the school day.

- The use by pupils of cameras in mobile phones is not permitted during or after school time. No pictures should be taken of staff or other children at out of school events organised by the school or the Parents' Association, such as discos and fetes. This also applies to parents. The school will investigate any reported cases of photos of staff or other pupils at such events being uploaded to social networking sites.

- At the headteacher's discretion, parents and carers are permitted to take pictures or videos of their own children at specified school events. If they wish to, parents and carers are permitted to upload photos onto social media as long as it is only of their own child.

b. Droxford Junior School Website

Our school web site is intended to:

- Provide accurate, up-to-date information about our school;
- Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- Celebrate good work;
- Provide pupils with the opportunity to publish their work on the internet;
- Promote the school.

It **may be used** to publish resources for projects or homework.

All classes **may** provide work for publication on the school web site. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. The administration assistant ensures that the links work and are up-to-date, and that the site meets the requirements of the site host.

The point of contact on the web site will be the school address, telephone number and e-mail address. We **do not publish pupils' full names or photographs that identify individuals** on our web pages. **Home information or individual e-mail identities will not be published**. Staff will be identified by their title and surname unless they request otherwise. **Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site**.

School Website Address: http://www.droxfordjunior.co.uk

c. Class Dojo

Class Dojo is intended as a quick and effective method of sharing work and successes, giving parents an insight into the school day and for communication between school and home. It can be used as an App or on an internet browser:

- Any messages to parents about topics which are not minor/celebrating successes (i.e. behaviour) should not be sent on Class Dojo – instead email these messages to parents via the admin office as usual.
- Parents are encouraged not to message school using Class Dojo unless they are replying to a teacher – parents should contact the admin office as usual with any messages.
- If a parent message teachers information that should be shared with the admin office, the teacher will send back a message advising such.
- If a parent's message are inappropriate or make a teacher feel uncomfortable, teachers should not message back and inform a member of SLT.
- Teachers are encouraged to turn off notifications for Class Dojo to preserve their work-life balance.
- To avoid 'spamming parents' with too many updates, teachers will send 2 or 3 messages to the class story each week as a maximum.
- Sometimes messages might be posted to the whole school story. These should be cleared with a member of SLT first.

d. Google Classrooms

Google Classrooms provides a new, cloud-based system for school work. Staff will be trained in the use of Google education products – either through staff meeting time with Harrap (our computer providers) or 1-to-1 with the school 'super admin'.

Using Google classrooms, teachers can share work and assignments with children, as well as send updates and resources. This can be used both at school and at home. It can be accessed via an App or on an internet browser:

- All teachers and children will have access to Google Classrooms via a google account linked to the school.
- Google Classrooms will be used in case of school closure to set and monitor home learning – see our Home Learning policy for how this will be used.
- Google Classrooms may also be used to set home learning when school has not been closed, and may be used in lessons.
- Parents/children are encouraged not to message school using Google Classroom unless they are replying to a teacher or relevant to the assignment

they are completing – parents should contact the admin office as usual with any messages.

- If a parent message teachers information that should be shared with the admin office, the teacher will send back a message advising such.
- If a parent's message are inappropriate or make a teacher feel uncomfortable, teachers should not message back and inform a member of SLT.
- While children can use their school google accounts at home, they should only do so to access or complete school work. Inappropriate usage may result in accounts being suspended.

Please see the Remote Learning Plan and the Home Learning E-Safety Policy for more details.

e. Twitter

Aim: To quickly share and celebrate children's achievements, successes and give parents up–to-date news and information. The following guidance applies:

- Only the Headteacher and selected staff with approval may 'tweet' updates using the school twitter account.
- The school Twitter account will be monitored by the ICT Leader and Headteacher.
- The school Twitter account will be a *Public account. Strategic leaders will monitor followers and block any who appear to not be school focused.*
- The school Twitter account will usually only tweet between the hours of 8am and 6pm between Monday and Friday. The only time tweets outside of this time are for school events (e.g. football matches, residential trips, performances) or to share urgent school news (e.g. closures due to adverse weather).
- The school Twitter account will only follow educationally or community linked accounts. No personal accounts, unless they are educationally linked (eg. a children's author), will be followed.
- The school Twitter account will not reply to any 'mentions' or 'replies' on Twitter. This is not the platform to discuss or debate school related issues.
- The school Twitter account will only not use names when referencing children – instead we will reference classes and yeargroups. eg. *Look at the fantastic Maths work from Meonstoke base this morning!*
- The school will use Twitter to share positive messages about the school.
- The school Twitter account will only post photos of children's for whom we have permission from parents. We may also tweet examples of school work and learning.
- The account may be used to share news and information during a school trip/school events. Photos taken on the phone for the purpose of sharing on Twitter will be deleted once they have been shared.
- The school will keep the Twitter account password secure.
- *Individually targeted content* will not be posted e.g. "Well done Josh a better lesson today".
- Twitter's own safety rules can be read on:

https://support.twitter.com/groups/33-report-abuse-or-policyviolations#topic_166

6. Monitoring

- The school uses Hampshire County Council's ICT services and therefore is required to comply with their email, internet and intranet policies.
- The school and county council reserve 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 school and county council's hardware, software, networks and systems are not compromised
- To prevent or detect crime or unauthorised use of the school or county council'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 school or county council may track the history of the internet sites that have been visited.
- To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

7. Communication with Parents, Pupils and Governors

The school 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. School must indicate to staff if any other staff are permitted to make contact using the systems below:

- School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the Senior Leadership Team where they feel they need to make a telephone call to a parent.
- Letters – normally all teachers may send letters home, but they may be required to have these approved by a member of the Senior Leadership Team before sending. Where office staff send letters home these will normally require approval by the School Business Manager/Administrative Officer.
- Email – when communicating with parents, teachers will copy in the admin office when appropriate. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

Under normal circumstances, school 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 Headteacher.

Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

8. Personal Information

School staff must never give out personal details of others or themselves, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the school's Data Protection Policies.

With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles.

9. Cyber Bullying and Harassment

a. This section should be read in conjunction with the guidance contained in "Cyber-bullying: Practical Advice for School Staff". Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim(s) is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

   The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work.

   Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

   It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the school's procedures. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182).

b. Cyber Bullying and Harassment: Pupils

The school will not tolerate any incidences of cyber bullying or harassment undertaken by any pupils using any of the school's ICT equipment. Any such incidences will be dealt with according to the school's Behaviour Policy. This may involve informing the parents/carers. Teachers may also consider whether access to the internet may be denied for a period.

As a school, we are aware that our pupils may experience cyber bullying or harassment at home from another pupil. This may take place over a variety of different media such as social networking, instant messaging or online gaming. The school will never condone cyber bullying or harassment regardless of where it takes place as it contravenes our school values. In the event of cyberbullying or harassment happening outside of school, we would urge the parents of the children involved to communicate with their children and each other to prevent any reoccurrences of this behaviour. This is the most effective way to deal with any such problems.

If any issues to do with cyber bullying or harassment outside of school spill over into the classroom and begin to affect children's health and safety at school, we will inform parents and discuss ways to manage the situation.

10. 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 Headteacher to such abuse. Where a concern relates to the Headteacher, 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) and may be recorded on CPOMS.

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

11. Senior Leadership Responsibility in Relation to Bullying and Harassment

The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment.

For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, or by any other means.

If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership Team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

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 School Social Media 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 Social Media may become a matter for police or social care investigations.

SharePoint Unique Identifier	HRDOCID-561776108-75764
Version and date of publication:	V1.4 July 2018 V 1.4.1 July 2019
Owner:	EPS

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

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, 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 school.

This Do's 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	Don't
- Ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources.	- Access or use any systems, resources or equipment without being sure that you have permission to do so.
- Ensure that where a password us required for access to a system, that it is not appropriately disclosed.	- Access or use any systems, resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for.
- Respect copyright and intellectual property rights.	- Compromise any confidentiality requirements in relation to material and resources accessed through ICT systems.
- Ensure that you have approval for any personal use of the school's ICT resources and facilities.	- Use systems, resources or equipment for personal use without having approval to do so.
- Be aware that the school's systems will be monitored and recorded to ensure policy compliance.	- Use other people's log on and password details to access school systems and resources.
- Ensure you comply with the requirements of the Data Protection Act when using personal data.	- Download, upload or install any hardware of software without approval.
- Seek approval before taking personal data off of the school site.	- Use unsecure removable storage devices to store personal data.
- Ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely.	- Use school systems for personal financial gain, gambling, political activity or advertising,
- Report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate.	- Communicate with parents and pupils outside of normal working hours unless absolutely necessary.
- Be aware that a breach of your school'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 bear due regard to your personal health and safety and that of others.	

Use of Email, the Internet, VLEs and School and HCC Intranets

Do	Don't
- Alert your Headteacher or designated manager is you receive inappropriate content via email.	- Send via email or download from email, any inappropriate content.
- Be aware that the school's email system will be monitored and recorded to ensure policy compliance.	- Send messages that could be misinterpreted or misunderstood.
- Ensure that your email communications are compatible with your professional role.	- Use personal email addresses to communicate with pupils or parents.
- 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 where messages are less open to misinterpretation) is more appropriate.	- Send messages in the heat of the moment.
- Be aware that the school may intercept emails where it believes that there is inappropriate use.	- Send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude.
- Seek support to block spam.	- Use email systems to communicate with parents or pupils unless approved to do so.
- Alert your Headteacher or designated manager if you accidentally access a website with inappropriate content.	- Download attachments from emails without being sure of the security and content of the attachment.
- Be aware that a website log is recorded by the school and will be monitored to ensure policy compliance.	- Forward email messages without the sender's consent unless the matter related to a safeguarding concern or other serious matter which much be brought to a senior manager's attention.
- Answer email messages from parents and parents within your directed time.	- Access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet.
- Mark personal emails by typing 'Personal/Private' within the subject header line.	- Upload any material onto the school website that doesn't meet style requirements and without approval.

Use of Telephones, Mobile Phones and Internet Messaging

Do	Don't
- Ensure that your communications are compatible with your professional role.	- Send messages that could be misinterpreted or misunderstood.
- Ensure that you comply with your school's policy on use of personal mobile telephones.	- Excessively use the school's telephone system for personal calls.
- Ensure that you reimburse your school for personal telephone calls as required.	- Use personal or school mobile phones when driving.
- Use school mobile telephones when on educational visits.	- Use the camera function on personal mobile telephones to take images of colleagues, pupils or of the school.

Use of cameras and recording equipment

Do	Don't
- Ensure that material recorded is for educational purposes only.	- Bring personal recording equipment into school without the prior approval of the Headteacher.
- Ensure that where recording equipment is to be used, approval has been given to do so.	- Inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded.
- Ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy.	- Put material onto the VLE, school intranet or intranet without prior agreement with a member of senior staff.
- Ensure that parental consent has been given before you take pictures of school pupils.	

Use of Social Networking Sites

Do	Don't
- Ensure that you understand how any site you use operates and therefore risks associated with using the site.	- Spend excessive time utilising social networking site while at work.
- Familiarise yourself with the processes for reporting misuse of the site.	- Accept friendship requests from pupils- you may be giving them access to personal information, and allowing them to contact you inappropriately.
- Consider carefully who you accept as friends on a social networking site.	- Put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial.
- Take care when publishing information about yourself and images of yourself online- assume that anything you release will end up in the public domain.	- Post anything that may be interpreted as slanderous towards colleagues, pupils or parents.
- Ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page.	- Use social media sites to contact parents and/or pupils.
- Follow school procedures for contacting parents and/or pupils.	
- Only contact pupils and/or parents via school based computer systems.	
- Through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role.)	

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 school'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 HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school 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 school 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 school'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 school, taken off the school premises or accessed remotely. I will not routinely 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 Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, 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 school’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-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school’s ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school’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 E-Safety, Social Networking and Acceptable Use of ICT Policy 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 any member of the Senior Leadership Team.

SIGNED:
…………………………………………………………………………………

DATE:……………………………………………………………………………...….

Legal and Policy Framework **Appendix 3**

The School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- General Data Protection Regulations (GDPR) 2016 and Data Protection Act 2018, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Copyright, Designs and Patents Act 1988.
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010

Related Policies

This policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- County Council Guidance on using Social Media
- Disciplinary Procedures
- Equalities Policy

Appendix 4: Code of Conduct for Internet and e-mail use for Pupils/Parents

Children at Droxford Junior School are responsible for their own good behaviour when using the Internet.

The Internet facilities provided by the school are for children and staff to use for research appropriate to their work. These facilities are a privilege, not a right. During school time, members of staff will offer guidance to students in search techniques and finding appropriate material.

Current policy is that children do not have access to e-mail facilities because of the security and safe monitoring issues.

The following activities are **not** permitted under any circumstances:

1. **Searching for, or displaying, offensive messages or images.**
2. **Sharing or sending offensive messages and images to others.**
3. **Any action likely to damage computers or other equipment.**
4. **Any attempt to transmit or download files without the permission of school staff.**
5. **Any action which violates copyright laws.**

- □ I will not access other people’s files or accounts.
- □ I will not send or share inappropriate messages or images.
- □ I will only use the computers/google accounts for school work and homework.
- □ I will not bring in USB sticks or other media from outside school unless I have been given permission.
- □ I will not change desktop settings or alter the school's computers in any way.
- □ When using the Internet, I will not visit inappropriate sites.
- □ I understand that the school will check my computer files and may monitor the Internet sites I visit.

Should any of these rules be broken or there be any other cause for concern, the school will take appropriate action against the offender(s). In extreme cases the police and/or other relevant authorities will be informed.

Both child and parent need to read and sign this section of the form and return to the school office.

Child Commitment

As a user of the Internet I agree to comply with the Internet Code of Conduct. I will use the Internet in a responsible way and I will observe the restrictions outlined in the Code of Conduct.

Name (block capitals)…………………………………………………………………………………..………..

Signature…………………………………………………..……..Class…………………..…Date………..……

Parent Statement

As the parent (or legal guardian) of the above child I give him/her permission to use the Internet and I have read and understood the above rules. I have discussed the implications of breaking them with my son/daughter.

Name (block capitals)…………………………………………………………………………………..………..

Signature…………………………………………….………………………………..…Date………..……..