Online Safety Policy

September 2019

Review Date: September 2020

Contents:

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Gascoigne Primary School with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Gascoigne Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Risks

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- Lifestyle websites, for example pro-anorexia/self-harm/suicide/extremist sites;
- Hate/extremist sites;
- Content validation: how to check authenticity and accuracy of online content;
- Grooming;
- Online bullying in all forms;
- Identity theft (including 'frape' (hacking social media profiles)) and sharing passwords;
- Privacy issues, including disclosure of personal information;
- Digital footprint and online reputation;
- Health and well-being (amount of time spent online (Internet or gaming);
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- Copyright (little care or consideration for intellectual property and ownership such as music and film).

Scope

This policy applies to all members of the Gascoigne Primary School community (including staff, pupils/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school computer systems, both in and out of Gascoigne Primary School.

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator/Officer • To ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures (e.g. ICT Network Manager)
Designated Safeguarding Lead	• takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies/documents • promotes an awareness and commitment to Online safeguarding throughout the school community • ensures that Online safety education is embedded across the curriculum • liaises with school computing technical staff • To communicate regularly with SLT and the designated Online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online safety incident log is kept up to date (secure Safeguarding Drive) • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal/inappropriate materials • inappropriate on-line contact with adults/strangers • potential or actual incidents of grooming

Role	Key Responsibilities
	• Online bullying and use of social med
Online safety governor	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include regular review with the Online Safety Co-ordinator/Officer (including online safety incident logs, filtering/change control log)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly
ICT Network Manager	• To report any online safety related issues that arise, to the online safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school IT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • To ensure that the school's policy on web filtering is applied and updated on a regular basis • To ensure that IT Provider is informed of issues relating to the filtering applied by them. • To ensure that he/she keeps up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To ensure that the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the Designated Safeguarding Lead for investigation. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures

Role	Key Responsibilities
	• To ensure that all data held on pupils is adequately protected • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • To ensure all networking services are managed on behalf of the school including maintaining the database of access accounts
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy • To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • To know and understand school policy on the taking/use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy

Role	Key Responsibilities
	covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/review of e-safety policies
Parent Liaison Officer	• To educate Parents and raising awareness as instructed by Headteacher.
Parents/carers	• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website/LEARNING PLATFORM/on-line pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy is posted on the school website/staffroom/classrooms
- Policy is part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling Complaints

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Discussion with the pupil about the incident with a senior member of staff or appropriate member of staff;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to Police.

Our Designated Safeguarding Leads act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

Review and Monitoring

The Online Safety Policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Improvement and Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

The school has Designated Safeguarding Leads who will be responsible for document ownership, review and updates. The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. The Online Safety Policy has been reviewed by the Designated Safeguarding Leads and is current and appropriate for its intended audience and purpose.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

1. Education and Curriculum

Pupil Online Safety Curriculum

Gascoigne Primary School has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE curriculum. It is built on online safeguarding and online literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;

- to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to
- understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music/video files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- to understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming/gambling;

Staff and Governor Training

Gascoigne Primary School:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program; termly staff meetings.
- Provides, as part of the induction process, all new staff [including those on
- university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent Awareness and Training

Gascoigne Primary School will run a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
- Information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe Internet use at home; (Parental control/Filtering)
- provision of information about national support sites for parents.

2. Expected Conduct and Incident Management

Expected Conduct

At Gascoigne Primary School, all users:

- are responsible for using the school computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on online bullying
- staff are responsible for reading the school's Online Safety Policy and using the
- school computing systems accordingly, including the use of mobile phones, and handheld devices.
- pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- parents/carers should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- use of parental controls & filtering

Incident Management

At Gascoigne Primary School:

- there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

3. Managing the IT and Computing Infrastructure

Internet Access, Security and Filtering

Gascoigne Primary School:

- Has the educational filtered secure broadband connectivity through Broadband4;
- Uses the Lightspeed filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, extremist sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the pupils;
- Ensures network healthy through use of Sophos anti-virus software and the network is set-up so staff and pupils cannot download and run executable files;
- Uses DfE & B&D approved systems such as S2S, Egress, secure email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes/Internet literacy lessons
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable/useful;

- Works in partnership with the staff to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment, secure platforms such as J2Bloggy, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct pupils to age/subject appropriate web sites; plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Yahoo for kids, Google Safe Search or Ask for kids.
- Never allows/is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the ICT Network Manager. Our ICT Network Manager logs or escalates as appropriate to the Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities Police – and the LA.

Network Management (User Access, Backup)

This school:

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful (RMTutor);
- Has additional local network auditing software installed (Elementary ICT Sherlock, Spiceworks);
- Ensures the network manager is up-to-date with services and policies.
- Storage of all data within the school will conform to the UK data protection requirements

Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes (Integris);
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 5 minutes and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 7 pm to save energy;
- Has set-up the network so that users cannot download and run executable files/programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health, Safety and Wellbeing is followed; e.g. projector filters cleaned by site manager/Technician; equipment installed and checked by approved suppliers/electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; Inclusions Manager - SEND data;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education

- Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files; Via Veeam.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system through secure file exchange (Egress);
- Follows ISP, LA and Elementary ICT advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors & Touchscreens are maintained so that the quality of presentation remains high;
- Reviews the school IT systems regularly with regard to health and safety and security.

Password Policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use a Strong password for access into our MIS system (Integris).
- We require staff to change their passwords into the MIS every 90 days and their Domain password every 60.

E-mail

Gascoigne Primary School:

- Provides staff with an email account for their professional use, Outlook 365 email and makes clear personal email should be through a separate account;
- Provides highly restricted/simulated environments for e-mail with Key Stage 1 pupils;

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@gascoigne.co.uk or group e-mail addresses (with one or more staff having access to an aliased/shared mailbox) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language, Finally, and in support of these, Lightspeed filtering monitors and protects our Internet access to the World Wide Web.

Pupils

Pupils are introduced to, and use e-mail as part of the IT/Computing scheme of work. Year R/1 pupils are introduced to principles of e-mail through the Visual Mail facility in the London LEARNING PLATFORM OR closed 'simulation' software. Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher/responsible adult if they receive an e- mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

Staff can only use the school provided Outlook 365 e-mail system. Staff only use e- mail systems for professional purposes. Access in school to external personal e mail accounts may be blocked. Never use email to transfer staff or pupil personal data. We use secure DfE approved systems. These include: S2S (for school to school transfer); Collect; Egress, Integris. Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house- style':

- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

All staff sign our school Agreement Form Acceptable Use Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: e.g. Network manager
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@gascoigne.co.uk Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved social media sites to password protect them and run from the school website.

Learning Platform

- Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;

Social Networking

Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications. The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils/pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school:

- Only uses the 3CX or Skype/Teams supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV

We have CCTV in the school as part of our site surveillance for staff and pupil safety. We will not reveal any recordings (*retained by the DVR/NVR for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation. We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

4. Data Security: Management Information System Access and Data Transfer

Strategic and Operational Practices

The Head Teacher is the Senior Information Risk Officer (SIRO). Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners. We ensure staff know who to report any incidents where data protection may have been compromised.

Our DPO is:
Craig Stilwell
dataservices@judicium.com
020 3326 9174

All staff are DBS numbers are held in one central record in the school's Admin Drive (restricted access).

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have an electronic system so we know who has signed. This includes:

- staff
- governors
- pupils
- parents

This makes clear staff responsibilities with regard to data security, passwords and access.

We follow DfE guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services.

We require that any Protected and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have no remote access system.

School staff with access to setting-up usernames and passwords for email, network access and SharePoint access are working within the approved system and follow the security processes required by those systems.

We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

<u>Technical Solutions</u>

- Staff have secure   areas   on   the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use OneDrive if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system to transfer admissions data.
- We use Egress to encrypt data if needed.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.

- All servers are in lockable locations and managed by DBS-checked staff.
- We the back-up Microsoft DPM server is in a locked server room. Back-ups are encrypted.
- We use Veeam for off site back-ups for disaster recovery.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder/collected by secure data disposal service.
- We are using secure file deletion software.

5. Equipment and Digital Content

Personal Mobile Phones and Mobile Devices

- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets and changing areas.
- Mobile phones brought into school are entirely at the staff member's, pupils & parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought intoschool.
- Pupil mobile phones which are brought into school must be turned off (not placed on silent) and handed to the office on arrival at school. They must remain there until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School Office. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their breaktimes.

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a senior member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

- Pupils' Use of Personal Devices

- The School strongly advises that pupil mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office and handed to the parent. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated and kept in the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile

- phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital Images and Video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins Gascoigne Primary School;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset Disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1

Acceptable Use Agreement (Pupils)

15 rules for responsible use
- I will STOP and THINK before I CLICK.
- I will verify information before accepting its true.
- I will be aware that the author of a website may be biased.
- I will be polite online and will not use bad or abusive language.
- I will keep personal information private.
- I understand how photographs can be manipulated and attract the wrong sort of attention.
- I understand online 'friends' may not be who they say they are.
- I will not share   my personal life, contact details, daily routines,   location, photographs or videos online.
- I will ensure privacy settings are turned on.
- I will not post pictures or videos of others without permission.
- I will not to download any files without permission.
- I will tell an adult if I receive inappropriate materials.
- I understand the impact of online bullying and know how to seek help.
- I will report any online bullying to an adult or by clicking the CEOP button.
- I will be SMART in online environments.

Pupil name:_____ Class:_____ Date: _____

Appendix 2

Acceptable Use Agreement (Staff)

Statement of Principles

The school makes a range of digital technologies available to staff for use in connection with their employment by the school, and for use in connection with professional activities that arise from their employment by the school.

Staff should not use the digital technologies provided by the school for activities that are illegal, or, for other reasons, incompatible with their professional role. This Acceptable Use Agreement covers staff use of digital technologies in school, e.g. email, Internet, intranet and network resources, SharePoint, software, equipment and systems.

As a person who works at Gascoigne Primary School, I agree that:

- I will only use the school's digital technology resources and systems for school and professional purposes;

- I will use the school email and telephone systems for school business only; I will not use a private email or telephone to conduct school business, unless instructed by the Head Teacher;

- I will not use the school's digital technologies for personal uses such as social media and buying/selling;

- I will not browse, download or send material that could be considered extremist, pornographic, obscene or offensive;

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/ ICT Network Manager;

- I will keep private my login/password(s) for school digital technologies and will not allow any other person to use my login/password(s)to access the school's digital technologies;

- I will not allow unauthorised individuals to access email/Internet/network, or other school systems;

- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed;

- I understand that all Internet usage/network usage and telephone usage can be logged and this information could be made available to SLT on request;

- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols;

- I will not connect a computer (or similar device) to the network/Internet without consent from the Network Manager and I will keep any 'loaned' equipment or BYOD (bring your own device) up-to-date, using the school's recommended anti - virus system;

- I agree and accept that any computer, laptop, iPad or mobile phone loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any 'significant personal use' that would deem the device a benefit as defined by HM Revenue & Customs.

- I will not connect a USB flash/HD drive to the school network without consent from the Network Manager;

- I will not use personal digital cameras or camera phones for transferring images of pupils or staff. Images will only be taken and used in accordance with the school's policy;

- I will use the school's SharePoint in accordance with school advice;

- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not in conflict with my professional role;

- I will not engage in any online activity that may compromise my professional responsibilities;

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location;

- I understand that data protection law requires that any personal information (e.g. staff or pupil records) will be kept private and confidential, and will only be used for the purpose for which it was collected/created. I will only share information with external organisations when authorised by the Head Teacher or designated member of staff. I will take every reasonable step to avoid accidental disclosure of confidential information (e.g. by keeping my login/password(s) for various school systems private);

- I will ensure I am aware of safeguarding approaches relevant to the use of digital media and will ensure they are embedded in my classroom practice by reading the e-safety policy, available on the school's website;

- I will only use LA systems in accordance with any council policies;

- I understand that accessing other users' mailboxes breaches the data protection act and their right to privacy; and that a detailed log of how and when such access is granted is kept.

- I understand that the school protects data as described in the E-Safety policy.

- I understand that failure to comply with this policy could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date, understand and abide by the school's most recent Acceptable Use Policy and E-Safety Policy. I wish to have an email account and a SharePoint login; access to the network and Internet and be able to use the school's ICT resources and systems.

Signature:_____Full Name: _____

Date: _____

Appendix 3

Letter to Parents: Electronic Consent

Dear parents/carers,

As part of our efforts to provide our pupils with a modern, engaging curriculum, they have access to a variety of trusted online resources during their learning time including iPad apps and web-based activities.

As part of their ICT programme of study, children regularly have discussions about keeping safe online and using all electronic equipment in an effective, responsible way in order to enhance their learning experiences.

Our school subscribes to a robust Internet filtering service which blocks any inappropriate sites. Our teaching staff constantly supervises all electronic usage and are always there to support pupils when needed, following local and national guidance.

Staff regularly monitor the children's files and web-based sites they visit and will contact you if any concerns were ever risen.

From time to time, the school may want to celebrate the pupils' achievements and work successfully completed via our website, our social media channels or local press with photographs which never identify the children by name and surname.

Our e-Safety policy can be accessed in more detail via our school website:
www.gascoigneprimaryschool.co.uk