

E-Safety Policy



School: Jigsaw Pupil Referral Unit

Date Approved by Management Committee:

Signed by Mr D. Hains

Date: Feb 22

Headteacher: E Rothlisberger

Review Date: Feb 23

Jigsaw E-Safety Policy

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

2. Education and Curriculum

- Pupil e-safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the ICT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
-

7. COVID-19 school closure arrangements for ICT & E-safety

- Children and online safety away from school
- Delivering Remote Lessons
- Reporting Concerns

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Jigsaw with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Jigsaw
- 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 cyberbullying 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 students.

The main areas of risk for our school community can be summarised as follows:

Content

- 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 sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- 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)
- (Ref Ofsted 2013)

Radicalisation and the Use of Social Media to encourage extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;
- accessing to likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Jigsaw Primary Pupil Referral Unit has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils
- Pupils, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Scope

This policy applies to all members of Jigsaw community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of Jigsaw.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / 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 cyber-bullying, or other e-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.

Jigsaw 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 e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> • To take overall responsibility for e-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 e-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. • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with Avarto technical staff • To communicate regularly with SMT and the designated safeguarding management committee member / committee to discuss current issues, review incident logs and filtering • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • 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: <ul style="list-style-type: none"> • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media

Role	Key Responsibilities
Management Committee / Safeguarding member	<ul style="list-style-type: none"> • To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Management committee / Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Management committee has taken on the role of Safeguarding • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety member will include: <ul style="list-style-type: none"> • regular review with the Headteacher (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader (PC)	<ul style="list-style-type: none"> • To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the Headteacher regularly
Agyllis technicians	<ul style="list-style-type: none"> • To report any e-safety related issue that arises, to the headteacher • 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 ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • 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 e-security and technical procedures
Teachers	<ul style="list-style-type: none"> • To embed e-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

Role	Key Responsibilities
All staff	<ul style="list-style-type: none"> • 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 e-safety issues related to the use of mobile phones, cameras and hand held 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 e-safety coordinator • To maintain an awareness of current e-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	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • 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 hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy 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
Parents/carers	<ul style="list-style-type: none"> • to support the school in promoting e-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 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

Role	Key Responsibilities
External groups	<ul style="list-style-type: none"><li data-bbox="411 271 1310 342">• 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 to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year or when the join Jigsaw.
- Acceptable use agreements to be issued to whole school community, usually 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 e-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:
 - interview/counselling by classteacher/ TA/Headteacher;
 - informing parents or carers;
 - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system.
 - referral to LA / Police.
- Our Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying 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 Headteacher will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school Headteacher and ICT co-ordinator 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 SMT and approved the Management Committee. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Title	Jigsaw e-safety policy
Version	1.0
Date	26/01/2022
Author	Paul Crawford/ Erika Rothlisberger
Approved by Governing Body	
Next Review Date	

Modification History			
Version	Date	Description	Revision Author

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has an e-safety education programme as part of the Computing curriculum / PSHE curriculum. 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 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 cyberbullying, sexting 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 cyberbullying; 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 students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school.
- 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 on-line; on-line gaming / gambling;

Staff and management committee training

This 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 e-safety issues and the school's e-safety education program
- 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.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT 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 e-safety practice when using digital technologies out of school and realise that the school's E-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 hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/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 e-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

Incident Management

In this school:

- There is strict monitoring and application of the e-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 in dealing with e-safety issues
- Monitoring and reporting of e 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 Management Committee

- Parents / carers are specifically informed of e-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

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through Sefton
- Uses Sefton's filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures staff and pupils cannot download executable files;
- Uses Sefton approved e-mail systems
- 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;
- 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 students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : eg the school's website
- Requires staff to preview websites before use [where not previously viewed or cached; 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](#) or [ask for kids](#) , Google Safe Search ,
- 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 students that that they must report any failure of the filtering systems directly to the teacher.
- 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 programme;
- 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.

To ensure the network is used safely, Jigsaw:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access (where appropriate) and network access.
- We provide pupils with an individual network log-in username.
- All pupils have their own username and password which gives them access to the network and the Internet.
- 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.
- 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.
- Has set-up the network so that users cannot download 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 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 and Safety is followed;
e.g. equipment installed and checked by approved Suppliers / LA 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;
- 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.
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- All computer equipment is installed professionally and meets health and safety standards;

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.

E-mail

Jigsaw

- Provides an email account for each class, the deputy, head and administrators for their professional use. Staff also have access to Sefton email accounts.
- 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 admin.Jigsaw@schools.sefton.gov.uk
- 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 technologies to help protect users and systems in the school, including desktop anti-virus, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, Sefton 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 ICT/Computing scheme of work.
- Pupils are taught about the 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 or 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 LA or schools e mail systems on the school system
- Staff only use LA or schools e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer);
- 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 LA / school Agreement Form AUP 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:
- 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. info@schooladdress or admin@schooladdress. 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

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

The recent upsurge in the popularity of social networking sites such as Facebook, Tik Tok, Instagram and Twitter requires schools to be aware of the potential dangers to staff and pupils. It has become much easier for individuals to publish content and information about themselves on the Internet. The risk of identity theft and the misuse of published photographic material should be considered as risks by all and appropriate steps to educate and protect staff and pupils be made.

- All social networking sites will be blocked in school.
- Consideration will be given, at all times, on how to educate pupils in their safe use.
- Pupils will be advised never to give out information that will identify themselves, their friends or their location.
- Pupils will be directed towards moderated sites.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be encouraged not to publish photographic content of themselves.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or Jigsaw/other 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 Jigsaw or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record
We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
 - staff,
 - management committee members,
 - pupils
 - parentsThis makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as SIMS 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 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.

Technical Solutions

- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- All servers are managed by DBS-checked staff.
- Paper based sensitive information is shredded

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones and hand held devices which are brought into school must be turned off and handed in to school staff. Staff members may use their phones during school break times. Except in extenuating circumstances, staff mobile phones should be kept in the office area. 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 restrict 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 hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. 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 break times.
- 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. pupil 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 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.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school. We recognise that pupils travel a distance by transport and may be allowed phones during journey. All devices are handed in on arrival at school and stored and returned at the end of the day.
- 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 student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a student 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.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

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 students, 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 students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then 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 students 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 the 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;
- 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 ICT 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 identify 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.

Context

During the current school closures due to Covid-19 there has been an unprecedented and rapid change to the expectations around ICT usage to support remote home learning.

7. Children and online safety away from Jigsaw

Jigsaw will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. Whilst staff are interacting with children away from the school, they must continue to adhere to the Jigsaw's Personal and Professional Conduct of Staff, Safe Working Practice Policy, ICT and E-Safety Policy and any other policies, protocols, professional standards and statutory guidance applicable to their role.

Staff should use parents' or carers' email addresses or phone numbers from the schools management information system (SIMs) to communicate relevant information about children, unless this poses a safeguarding risk. Use work accounts to communicate via email or online platforms, never use personal accounts. All remote communication with students should be done exclusively via approved IT platforms.

In light of our change in practice due to COVID19, it may be necessary for staff to use their personal mobile phones to communicate with students, parents and carers. Where this is deemed necessary, this must be agreed by a member of the Leadership Team. Where applicable, staff should make sure any phone calls from a personal device are made from a blocked number, so personal contact details are not visible. Keying 141 before the phone number will block your caller ID on the call you are making.

If staff members are accessing families' contact details at home, ensure they comply with the Data Protection Act 2018.

Children and young people are likely to spend more time online due to social distancing. Talk to them regularly about the benefits and risks of the online world and give them space to ask questions and talk about anything that worries them.

Delivering Remote Lessons

We are currently not delivering either recorded or live lessons, but would be aware of the following procedures should this change.

- Remote 1:1's with students should be avoided, with students being tutored in groups wherever possible. If this is unavoidable, this must be approved by the Head of School.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach Jigsaw policies
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.

- Language must be professional and appropriate, including any family members in the background.
- Staff should monitor any class peer to peer conversations through remote learning platforms where possible.
- Staff must only use platforms specified and approved by senior managers to communicate with pupils.
- Staff should record the length, time, date and attendance of any sessions held.
- Consider activities carefully when planning – online access within school has internet content filtering systems in place that are unlikely to be replicated in the home environment.
- Be careful that staff and children don't incur surprising costs, eg mobile data access charges - (video utilises significant amounts of data).

Reporting Concerns

Communicating online may allow you a view into a young person's world that you would not have seen before (and would maybe not have had the opportunity to without this crisis). This may also generate some safeguarding concerns for that young person. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Any concerns must be recorded and monitored on CPOMS and a Designated Safeguarding Lead (DSL) must be informed immediately.

You will also notice if a child is not engaging in learning as required. Where this is the case, this must be reported to a member of the Leadership team so that contact can be made with the child and parent/carer, after an agreed period of time to ensure they are safe and well. Any continued concerns must be referred to the relevant organisations to ensure the safeguarding of the child.