The Willows School
Academy Trust
Learning - Achieving - Succeeding

# I.C.T. Policy

**This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.**

**Contents**

2. A2: Acceptable Use Agreement for Staff
3. A3: Protocol for handling infringements
4. A4: Guidelines “What to do if...”

## 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 The Willows School Academy Trust with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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:**

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation

- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

## Scope

This policy applies to all members of the The Willows School Academy Trust's community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of The Willows School Academy Trust's IT systems, both in and out of the school.

## Roles and responsibilities

| Role | Key Responsibilities |
|---|---|
| Headteacher | • Must be adequately trained in off-line and online safeguarding, in- line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance<br><br>• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.<br><br>• To take overall responsibility for online safety provision<br><br>• To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling<br><br>• To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services<br><br>• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles<br><br>• To be aware of procedures to be followed in the event of a serious online safety incident<br><br>• Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised |

| | |
|---|---|
| | • To receive regular monitoring reports from the Online Safety Co- ordinator<br><br>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager<br><br>• To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety<br><br>• To ensure the school website includes relevant information. |
| Online Safety Co-ordinator | • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents<br><br>• Promote an awareness and commitment to online safety throughout the school community<br><br>• Ensure that online safety education is embedded within the curriculum<br><br>• Liaise with school technical staff where appropriate<br><br>• To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs<br><br>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident<br><br>• To ensure that online safety incidents are logged as a safeguarding incident<br><br>• Facilitate training and advice for all staff<br><br>• Oversee any pupil surveys / pupil feedback on online safety issues<br><br>• Liaise with the Local Authority and relevant agencies<br><br>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.<br><br>• To ensure the delivery of the online safety element of the Computing curriculum |

| | |
|---|---|
| Governors / Safeguarding Governor | • To ensure that the school has in place policies and practices to keep the children and staff safe online<br><br>• To approve the Online Safety Policy and review the effectiveness of the policy<br><br>• To support the school in encouraging parents and the wider community to become engaged in online safety activities<br><br>• The role of the safeguarding Governor will include a regular review with the online safety Co-ordinator |
| Network Manager / Technician | • To report online safety related issues that come to their attention, to the Online Safety Coordinator<br><br>• To manage the school's computer systems, ensuring<br><br>○ school password policy is strictly adhered to. systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)<br>○ access controls/encryption exist to protect personal and sensitive information held on school-owned devices<br>○ the school's policy on web filtering is applied and updated on a regular basis<br><br>That they keep 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<br><br>That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher<br><br>To ensure appropriate backup procedures and disaster recovery plans are in place<br><br>To keep up-to-date documentation of the school's online security and technical procedures |

| | |
|---|---|
| Data Controller(s) | • To ensure that the data managed is accurate and up-to-date<br><br>• Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.<br><br>• The school must be registered with Information Commissioner |
| LGfL Nominated contact(s) | • To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant |
| Teachers | • To embed online safety in the curriculum<br><br>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)<br><br>• 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, volunteers and contractors. | • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction.<br><br>• To supervise pupils carefully when using online technology (including, extra-curricular and extended school activities if relevant)<br><br>• To report any suspected misuse or problem to the online safety coordinator<br><br>• To maintain an awareness of current online safety issues and guidance e.g. through CPD<br><br>• To model safe, responsible and professional behaviours in their own use of technology<br><br>• At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and |

| | |
|---|---|
| | technician on the last day to log in and allow a factory reset. |
| Pupils | • Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually<br>• To understand the importance of reporting abuse, misuse or access to inappropriate materials<br>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology<br>• To understand the importance of adopting safe behaviours and 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<br>• To contribute to any 'pupil voice' / surveys that gathers information of their online experiences |
| Parents/carers | • To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren<br>• To consult with the school if they have any concerns about their children's use of technology<br>• 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 |
| External groups including Parent groups | • Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school<br>• To support the school in promoting online safety<br>• To model safe, responsible and positive behaviours in their own use of technology. |

The School Online Safety Coordinator is **Paul Gregory-Hunt and Malcolm Shaw**. The Online Safety coordinator should also act as a central point of contact for all Online Safety issues within the school, ensuring that policies

are in place, current and adhered to, instances of breaches and misuse are monitored and reported, and that all staff receive relevant information.

**Communication:**

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

- Policy to be posted on the school website.
- Key Reminders to be posted in all classrooms, computing room and areas or the school where computing technology is used
- Policy and Key Reminders to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements to be issued to whole school community, on entry to the school.
- Acceptable use agreements signed by staff and discussed and agreed pupils at the start of each year.
- Parents and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.
- The school will maintain a list of Online Safety resources for parents/carers which will be highlighted on the website and at periodical Online Safety information.

**Handling Incidents:**

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

**Handling Online Safety complaints**

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure (see school's complaints policy). Pupils and parents will be informed of consequences for pupils misusing the internet and incidents will be dealt with under the school's behaviour policy.

**Review and Monitoring**

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Behaviour policy, PSHE).

- The online safety policy will be reviewed biennially or when any significant changes occur with regard to the technologies in use within the school

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

## 2. Education and Curriculum

### Pupil online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the computing and SMSC and ICT curriculum. This covers a range of skills and behaviours appropriate to their age and experience;

- Plans online 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 the pupil Acceptable Use Agreement(s);

- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;

- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

- Ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

**Staff and governor training**

This school:

- Makes regular training available to staff on online safety issues and the school's online 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 Online Safety Policy and the school's Acceptable Use Agreements.

**Parent awareness and training**

This school:

- Runs a rolling programme of online safety advice, guidance and training for parents, including periodical Online Safety information evenings.

## 3. Expected Conduct and Incident management

**Expected conduct**

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;

- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;

- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;

- Know and understand school policies on the use of mobile and hand held devices including cameras;

**Staff, volunteers and contractors**

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

**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;

- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

**Incident Management**

In this school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- All members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;

- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;

- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;

- MASH and/or the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;

- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

## 4. Managing IT and Communication System

### Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;

- Has the educational filtered secure broadband connectivity through the LGfL;

- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;

- Uses USO user-level/assigned IP range filtering where relevant (e.g. for Youtube);

- ensures network health through use of Sophos anti-virus software (from LGfL);

- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2 to send 'protect-level' (sensitive personal) data over the Internet

- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

**Network management (user access, backup)**

This school

- Uses individual, audited log-ins for all users (e.g. the LGfL USO system);

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;

- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;

- Has daily back-up of school data (admin and curriculum);

- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data 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.

- Pupils group have their username and password which gives them access to the Internet and other services;

- 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;

- 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 log off when they have finished working or are leaving the computer unattended;

- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.

- Maintains equipment to ensure Health and Safety is followed;

- Ensures that access to the school's network resources from remote locations by staff is audited and restricted

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;

- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- This school uses secure data transfer; this includes 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 in our LA or through USO secure file exchange (USO FX);

- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

**Password policy**

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

- We require staff to change their passwords regularly into the MIS, LGfL USO admin site.

- We require staff using critical systems to use two factor authentication. **E-mail**

**This school**

- Provides staff with an email account for their professional use, London Staffmail, and makes clear personal email should be through a separate account;

- 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

- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

**Pupils:**

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

**Staff:**

- Will use LGfL e-mail systems for professional purposes

- Know that access in school to external personal e mail accounts may be blocked

- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

**School website**

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- The school web site complies with statutory DFE requirements;

- 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;

- 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;

**Social networking**

**Staff, Volunteers and Contractors**

- Staff are instructed to always keep professional and private communication separate.

- 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.

**School staff will ensure that in private use:**

- No reference should be made in social media to students/pupils, parents/carers or school staff;

- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.

- 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 /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

**Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

**Parents:**

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

**CCTV**

- We may use 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.

## 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).

- Staff are clear who are the key contact(s) for data protection and key school information is (the Data Controller).

- 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 a single central record

### Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.

- All servers are in lockable or secure locations and managed by DBS-checked staff.

- Details of all school-owned hardware will be recorded in a hardware inventory.

- 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.

- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

## 6. Equipment and Digital Content

### Students' use of personal mobile devices

- Students may have permission to bring in equipment for their journey to and from the school.

- Any such student mobile devices brought into school must be turned off (not placed on silent) and be handed in to the admin office.

- Mobile devices brought in to school at the risk and responsibility of the device owner and the School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

- 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.

**Cyberbullying**

- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects.

- There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006to every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

- Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

- All incidents of cyberbullying reported to the school will be recorded using the school's serious incident records.

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Sanctions for those involved in cyberbullying may include:

    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti- bullying statement and behaviour policy.
    - Parents/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

**Staff/visitors use of personal devices**

- Mobile devices brought into school are entirely at the staff member or visitors own risk and the School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.

- Mobile Phones and personally-owned devices will be switched off or switched to ‘silent’ mode. Bluetooth communication should be ‘hidden’ or switched off during all lesson times or when supervising pupil activities in school, and should never be in use or out when with children (unless for a specific school activity where permission has been granted by a member of the senior leadership team).

- 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.

- Staff/visitors/volunteers 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.

- Mobile phones/devices should never be present when children are changing and should not be used to take photos within school or on school trips.

- Mobile Phones should be switched off or on silent during all lesson times or when supervising pupil activities in school, and should never be in use or out when with children (unless for a specific school activity).

- Parent volunteers/helpers are not permitted to take photographs of children for any purpose. When attending as audience, parents are welcome to take videos and photographs of school events for their own use. Parents are informed that for child protection and data privacy reasons (and copyright in the case of film), no image or film can be transmitted or published electronically (e.g. uploading Youtube clips, making online photo albums or sending email attachments) if it contains children other than their own child.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

- If a member of staff breaches the school policy then disciplinary action may be taken.

**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 (or annually).;

- 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;

- For the school website and marketing materials, photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full -face photos of individual children should be used wherever possible. Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs. Pupils in photographs should always be appropriately clothed. Pupil image file names will not refer to the pupil by name.

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment;

- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their online 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 computing 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendices:

1. A1: Acceptable Use Agreement (Staff, Volunteers and Governors)
2. A2: Acceptable Use Agreements (Pupils – adapted for phase)
3. A3: Acceptable Use Agreement including photo/video permission (Parents)
4. A4: Protocol for responding to online safety incidents http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements http://www.digitallyconfident.org/images/resources/first-line-information-support- HQ.pdf - page 23 onwards
5. A5: Prevent: Radicalisation and Extremism
6. A6: Data security: Use of IT systems and Data transfer

   Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation

**Appendix 1 – Pupil Acceptable Use Agreements**

Think before you click

S **I will only use the Internet and email with an adult**

A **I will only click on icons and links when I know they are safe**

F **I will only send friendly and polite messages**

E **If I see something I don't like on a screen, I will always tell an adult**

My Name:

**I will only use the Internet and email with an adult**

**I will only click on icons and links when I know they are safe**

**I will only send friendly and polite messages**

**If I see something I don't like on a screen, I will always tell an adult**

My Signature:

**Key Stage 1: Acceptable Use Agreement**

I keep **SAFE online** because ...
I **CHECK** it's OK to use a website / game / app.
I **ASK** for help if I get lost online.
I **THINK** before I click on things.
I **KNOW** online people are really strangers.
I am **RESPONSIBLE** so never share private information. I am **KIND** and polite online.
I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

✓□

……..

……..

Teacher

My name: Date signed:

**KS2 Pupil Online Acceptable Use Agreement**

***This agreement will help keep me safe and help me to be fair to others.***

- ***I am an online digital learner*** – I use the school's IT for schoolwork, home learning and other activities approved by trusted adults.

- ***I am a secure online learner*** - I keep my logins and passwords secret.

- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.

- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.

- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.

- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.

- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.

- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.

- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.

- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.

- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

- ***I know who my trusted adults are***

**I have read and understood this agreement.**

Signed:

Date:

**Appendix 2 – Staff Acceptable Use Agreement**

**Staff IT Acceptable Use Agreement**
Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.** These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

- I will not reveal my password(s) to anyone.

- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any Local Authority (LA) system I have access to.

- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.

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

- I will only use the approved email system(s) for any school business.

- I will not support or promote extremist organisations, messages or individuals. I will not give a voice or opportunity to extremist visitors with extremist views. I will not browse, download or send material that is offensive or of an extremist nature.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the headteacher.

- I will not download any software or resources from the Internet, including browser toolbars that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the school network.

- I will follow the school's policy on use of mobile phones/devices at school contained in the online Safety Policy.

- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

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

- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption ( for example by using encrypted memory sticks) and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the school's designated safeguarding lead.

- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the headteacher on their request.

- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

- I will only use any local authority system I have access to in accordance with their policies.

- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital extremism curriculum into my teaching.

*I agree to abide by all the points above. I understand that I have a responsibility for my own and others' e- safeguarding and I undertake to be a 'safe and responsible digital technologies user'. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding*

*policies. I understand that failure to comply with this agreement could lead to disciplinary action.*

Signed: .....

Print name: ..... Date: .....

## Appendix 3 – Protocols for Handling Infringements

### How will infringements be handled?

Whenever a student or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school leadership and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

| **STUDENT** | |
|---|---|
| **Category A infringements** | **Possible Sanctions:** |
| • Use of non-educational sites during lessons<br><br>• Unauthorised use of email<br><br>• Unauthorised use of mobile phone (or other new<br><br>technologies) in lessons e.g. to send texts to friends<br><br>• Use of unauthorised instant messaging / social networking sites | **Refer to class teacher**<br><br>Escalate to: senior leader |
| **Category B infringements** | **Possible Sanctions:** |
| • Continued use of non-educational sites during lessons after being warned<br><br>• Continued unauthorised use of email after being warned<br><br>• Continued unauthorised use of mobile phone (or other<br><br>new technologies) after being warned<br><br>• Continued use of unauthorised instant messaging /<br><br>chatrooms, social networking sites, NewsGroups<br><br>• Use of Filesharing software e.g. Napster, Vanbasco,<br><br>BitTorrent, LiveWire, etc<br><br>• Trying to buy items online<br><br>• Accidentally corrupting or destroying others' data without<br><br>notifying a member of staff of it<br><br>• Accidentally deleting or moving folders on the network | **Refer to Class teacher/ Senior Leader**<br><br>Escalate to:<br><br>Consider removal of Internet access rights for a period / contact with parent |

| | |
|---|---|
| • Accidentally accessing offensive material and not logging off or notifying a member of staff of it | |

| **STUDENT** | |
|---|---|
| **Category C infringements** | **Possible Sanctions:** |
| • Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site.<br><br>• Deliberately or repeatedly deleting or moving folders on the network<br><br>• Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)<br><br>• Trying to access offensive or pornographic material (one-off)<br><br>• Purchasing or ordering of items online<br><br>• Transmission of commercial or advertising material | **Refer to Class teacher / Online- Safety Coordinator / Head teacher**<br><br>Escalate to: contact with parents / removal of IT privileges for a period<br><br>**Other safeguarding actions**<br><br>**if inappropriate web material is accessed:**<br>Ensure appropriate technical support filters the site |
| **Category D infringements** | **Possible Sanctions:** |
| • Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned<br><br>• Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent<br><br>• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988<br><br>• Bringing the school name into disrepute | **Refer to Head Teacher / Contact with parents**<br><br>**Other possible safeguarding actions:**<br><br>• Secure and preserve any evidence<br><br>• Inform the sender's e-mail service<br><br>provider.<br><br>• Liaise with relevant service<br><br>providers/ instigators of the |

| | |
|---|---|
| | offending material to remove<br><br>• Report to Police / CEOP where<br><br>child abuse or illegal activity is suspected |

| **STAFF** | |
|---|---|
| **Category A infringements (Misconduct)** | **Possible Sanctions:** |
| • • Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.<br>• • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.<br>• • Not implementing appropriate safeguarding procedures.<br>• • Any behaviour on the World Wide Web that<br><br>compromises the staff members professional standing in<br><br>the school and community.<br><br>• • Misuse of first level data security, e.g. wrongful use of<br><br>passwords.<br><br>• Breaching copyright or license e.g. installing unlicensed<br><br>software on network. | **Referred to line manager / Head teacher**<br><br>Escalate to:<br><br>*Warning given* |
| **Category B infringements (Gross Misconduct)** | **Possible Sanctions:** |

| | |
|---|---|
| • Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;<br><br>• Any deliberate attempt to breach data protection or computer security rules;<br><br>• Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;<br><br>• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;<br><br>• Bringing the school name into disrepute | **Referred to Head teacher / Governors;**<br><br>**Other safeguarding actions:**<br><br>• Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.<br>• Instigate an audit of all IT equipment by an outside agency, such as the schools IT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.<br>• Identify the precise details of the material.<br><br>*Escalate to: report to LA /LSCB, HR.*<br><br>Report to Police / CEOP where child abuse or illegal activity is suspected. |

| |
|---|
| **If a member of staff commits an exceptionally serious act of gross misconduct**<br><br>The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.<br><br>Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Governing Body. |
| **Child abuse images found**<br>In the case of Child abuse images being found, the member of staff should be **immediately suspended**<br><br>and the Police should be called.<br><br>Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):<br><br>http://www.ceop.gov.uk/reporting_abuse.html http://www.iwf.org.uk |

**How will staff and students be informed of these procedures?**

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement;

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online- safety / acceptable use agreement form;

- The school's online-safety policy will be made available and explained to parents, and parents

will sign an acceptance form when their child starts at the school.

- Information on reporting abuse / bullying etc. will be made available by the school for pupils,

staff and parents.

- Staff are also issued with the 'What to do if?' guide on online-safety issues.

**Appendix 4 – Guidelines on "What to do if..."**

**Guidance: What do we do if?**

**An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.

2. Report to the head teacher and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: **Atomwide via the LGFL Helpdesk**).
4. Inform LGFL IT manager.

**An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform LGFL IT manager.

**An inappropriate website is accessed intentionally by a staff member.**

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. Inform LGFL Schools IT manager.
6. In an extreme case where the material is of an illegal nature:

a. Contact the local police and follow their advice.

**An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:

   Remove the device to a secure place.

4. Instigate an audit of all ICT equipment by the school's ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
5. Identify the precise details of the material.
6. Take appropriate disciplinary action (undertaken by Headteacher). Inform governors of the incident.

   In an extreme case where the material is of an illegal nature:

- Contact the local police and follow their advice.
  If requested to remove the device to a secure place and document what you have done.

All of the above incidents must be reported immediately to the head teacher.

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online-safety anti-bullying and SMSC and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, LGFL)

**Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LBH and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LGFL and other agencies.
6. Consider delivering a parent workshop for the school community.

**You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child**

1. Report to and discuss with the named child protection officer in school and contact parents.

2. Advise the child and parents on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents.

3. If the game is played within school environment, ensure that the technical team block access to the game

4. Consider the involvement social services and child protection agencies.

5. Consider delivering a parent workshop for the school community.

**You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.**

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher.

**Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology:**
**they must be able to do this without fear. The Willows School Academy Trist operates a no-blame culture.**