# BURLINGTON INFANT AND NURSERY SCHOOL

## POLICY TITLE: Online Safety Policy (eSafety)

**Persons with Responsibility:**
Michelle Docwra Inclusion Manager, Katherine Wilkinson Computing Coordinator with Claire McEvoy

**Key Legislation:**

**Documents consulted:**
LGfL Online Safety model policy for schools (Nov 2016)
Safeguarding and Child Protection Policy (2016)
Anti-Bullying Policy (2016)
PSHE Policy (2016)

**Policy History:**

| Issue No. | Date | Author | Summary of Changes | Next Review Date |
|---|---|---|---|---|
| 1 | March 2017 | SYW | | Spring 2020 |
| 2 | November 2020 | SH | Computing curriculum | Autumn 2023 |
| 3 | February 2024 | KW | | Spring 2027 |

**Approved by Governors at a meeting on: _____**

**Please refer to signed minutes of this meeting**

**Introduction**

This policy applies to all staff, students, volunteers, parents/carers, visitors, community users working in the school, who have access to and are users of our school's IT systems, both in and out of Burlington Infant and Nursery School (BINS).

**Aims of this policy**

1. To set out the key principles expected of all members of the school community at BINS with respect to the use of IT-based technologies.
2. To safeguard and protect the children and staff.
3. 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.
4. Set clear expectations of behaviour and practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community, which adheres to the relevant **Acceptable Use Agreements**.
5. Have clear structures to deal with online abuse, such as online bullying in conjunction with the school's Anti-Bullying and Safeguarding Policies. This includes reporting abuse, misuse or access to inappropriate materials.
6. 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.
7. Minimise the risk of misplaced or malicious allegations made against adults who work with students

**Communication of this policy:**

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

- Policy to be posted on the school website for parents/carers and Safeguarding notice board for all staff.
- Policy to be part of school induction pack for new staff, volunteers and students.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements shared with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

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

**Content** including exposure to inappropriate content such as 'Lifestyle' websites promoting harmful behaviours, 'Hate' content, 'Content validation' - how to check authenticity and accuracy of online content.

**Contact** including 'Grooming' (sexual exploitation, radicalisation etc.), 'Online bullying' in all forms, social or commercial identity theft, including passwords.

**Conduct** including 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' also referred to as SGII (Self-generated indecent images) Copyright (little care or consideration for intellectual property and ownership).

**Roles and 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
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.
- To take overall responsibility for online safety provision
- To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling
- To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services
- To be responsible for ensuring that all staff receive suitable regular training on online safety issues to carry out their safeguarding and online safety roles.
- To provide, as part of the induction process, all new staff/volunteers with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.
- To be aware of procedures to be followed in the event of a serious online safety incident.
- Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised as and when needed.
- To receive regular monitoring reports from the Online Safety Co-ordinator (from Data Protection Team).
- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. Data Protection Team and Coombe IT Support.
- To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- To ensure school website includes relevant information.
- To provide a rolling programme of online safety advice, guidance and training for parents on a regular basis. This includes the induction of new parents into the school.
- To take overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. This responsibility is delegated to the Communications Officer.

**Designated Safeguarding Lead**

- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents
- Promote an awareness and commitment to online safety throughout the school community
- Ensure that online safety education is embedded within the curriculum
- Liaise with school technical staff where appropriate
- To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- To ensure that any online safety incidents/concerns are logged as a safeguarding incident using the school's usual reporting procedures for safeguarding
- Facilitate training and advice for all staff
- Oversee any pupil surveys / pupil feedback on online safety issues
- Liaise with the Local Authority and relevant agencies
- Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
- ensure staff how know to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection and use password protected storage devices where necessary.

**Governors/Safeguarding governor**

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve the Online Safety Policy and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in online safety activities
- The role of the online safety Governor will include: regular review with the online safety Co-ordinator.

**School Business Manager and Network Manager/technician**

- To report online safety related issues that come to their attention, to the Headteacher
- To manage the school's computer systems, ensuring:
    - 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)
    - 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 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.
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Headteacher

- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the school's online security and technical procedures
- 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.
- To ensure that the school is registered with Information Commissioner
- Provide staff with an email account for their professional use
- Inform all users that Internet/email use is monitored
- Ensure that the school 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 the administrator with the approved 'web filtering management' status.
- To ensure that all appropriate staff use the USO user-level filtering where relevant.
- To ensure network health through use of anti-virus software.
- Uses DfE or LA approved systems (USO) to send 'protect-level' (sensitive personal) data over the Internet.
- To ensure all staff use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

**Computing lead**

- To oversee the delivery of the online safety element of the Computing curriculum
- To liaise with staff to keep this up to date and relevant and ensure staff feel confident in delivering it.
- To ensure that all data held on pupils on our learning platform (where there is one) is adequately protected
- To liaise with DPO to ensure we are GDPR compliant.

**School Business Manager/Systems Administrator (user access, backup)**

The school uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.

- Key staff members/Teachers may use 'remote access' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful.
- The SBM/Systems Administrator ensures the Technical Support Provider to be up-to-date with LGfL services and policies, and takes advice and carries out actions accordingly.
- Ensures the school 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.
- Ensure the network is used safely, by ensuring all staff read and sign that they have understood the school's Online Safety Policy.
- Sets staff up with internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.
- Ensures that the network has been set-up 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. All users are required 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, laptop or mobile device loaned to them by the school, is used primarily to support their professional responsibilities. Staff sign a user agreement form when loaning a device from the school.
- Ensures that the school has a clear disaster recovery system in place that includes a secure, remote off site back up of data.
- Oversees the school's use of a secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools. Our wireless network has been secured to appropriate standards suitable for educational use. All IT and communications systems have been installed professionally and regularly reviewed to ensure they meet health and safety standards.
- **Exit strategy:** At the end of the period of employment the SBM ensures that staff 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 login and allow a factory reset.
- **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 use STRONG passwords. We require staff to change their passwords into the MIS, LGfL USO admin site, twice a year. We require staff using critical systems to use two factor authentication.
- **Technical Solutions:** There are secure area(s) on the network to store sensitive files. All servers are in lockable locations and managed by DBS-checked staff. 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.

**Teachers, staff, volunteers**

- To embed online safety in the curriculum through a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience.
- 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.
- To remind students about their responsibilities through the pupil Acceptable Use Agreement(s).
- 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;
- To ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy and the Confidentiality Agreement at the start of each year, and understand any updates annually. The AUP is signed by new staff on induction.

- To ensure that personal mobile devices are not used during lessons or formal school time. They should be switched off or silent at all times. 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.
- To ensure that personal mobile phones or devices are not used in a professional capacity, such as for contacting parents within or outside of the setting. In an emergency where a staff member doesn't have access to a school-owned device (e.g. on a school trip or during lockdown), they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. If a member of staff breaches the school policy then disciplinary action may be taken.
- To only use school cameras/tablets to record children's work and store photographs of children on the shared Teacher drive on the school's server. Stored photographs should be deleted after one year after the child has left the school. Photographs and recordings of children must not be kept on mobile storage devices or removed from the school premises, unless in exceptional circumstances, e.g. to give to the child's parent.
- To ensure that no reference is made in social media to pupils, parents/carers with regard to any school related matters. Staff must not engage in online discussion on personal matters relating to members of the school community.
- To ensure that personal opinions are not attributed to the school or local authority and personal opinions do not compromise the professional role of any staff member, nor bring the school into disrepute.
- To understand that school staff must not be online friends with any pupil. There are no exceptions.
- To report any suspected misuse or problem to the online safety coordinator
- To report any concern about staff misuse directly to the Headteacher, unless the concern is about the Headteacher in which case it must be reported to the Chair of Governors/Safeguarding Governor and the LADO (Local Authority's Designated Officer). Any incidents involving 'Sexting' or nude selfie incident, should be handled by a DSL and must refer to **Appendix 1, 'Handling a sexting/nude selfie incident'**.
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To always maintain professional and private communication separate. Staff/volunteers must never post or share any school related matters, photographs or recordings on any social media sites. All staff/volunteers must adhere to the terms of the Confidentiality Agreement signed at the start of each year.
- 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.
- To only use the LGfL email systems on the school system, and for professional purposes.
- To ensure that emails are never used to transfer staff/pupil personal data ('Protect-level' data). If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.
- Ensures that no one should log on as another user and makes clear that pupils are never allowed to log-on or use teacher and staff logins.

**Curriculum at Burlington**

Teaching and learning at Burlington:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. 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 (fact, opinion, fiction)
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand that if it is unacceptable offline it is unacceptable online
- 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 without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- to understand the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff.
- Will remind students about their responsibilities through an end-user Staying Safe Online agreement (SSO) which every child will agree to and will be displayed throughout the school, through the website and on Tapestry.
- 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 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;

**Parents/carers/external groups or individuals**

- Are asked to read, adhere to and promote the school's Acceptable Internet and Technology Use Agreement with their child/ren.
- Are invited to attend the school's eSafety training for parents every year.
- Are advised on parental control settings for devices through the eSafety training and newsletters.
- Parents should consult with the school if they have any concerns about their children's use of technology to support the school in promoting online safety.
- Any external individual/organisation will also sign an Acceptable Use agreement prior to using technology or the Internet within school.
- Parents are asked to provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form.

- Are asked to sign Photograph permission slips in induction packs, for staff to take photographs and recordings of children's work and progress, when their child joins the school.
- **Parents may be permitted to take photographs and recordings at significant school events such as school productions and concerts. However, in order to safeguard all our children parents are reminded that images of other children are not to be posted on any social media websites at any time.**

**Pupils**

- Participate in lessons related to internet safety and responsible use of IT, as appropriate to their age and level of understanding.
- Pupils are taught to report anything that worries them in relation to internet safety, e.g. abuse, misuse or access to inappropriate materials. They should inform a teacher or member of staff if they or someone they know feels worried or vulnerable when using online technology.
- The school supports pupils to adopt 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.
- All pupils contribute to termly 'pupil voice' / surveys that gathers information about their safety and wellbeing at school, including their online experiences.

**Digital Images, Video and the School Website**

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs. Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/ personal equipment for taking pictures of pupils. If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will check that permission slips have been signed.
**The school website** 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.

**Appendix 1**

**Handling a sexting / nude selfie incident:**

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken. There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  *When assessing the risks the following should be considered:*
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to SPA and/or the police
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (e.g. special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupils are at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

## e-safety 'Acceptable Use Agreement' form: parents

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

**Use of digital images, photography and video:** I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

**Social networking and media sites:** I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

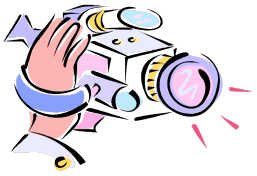
I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

**My daughter / son name(s): _____**

**Class : _____**

**Parent / guardian signature: _____**

**Date: ___/___/___**



# The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

**If the pupil is named, we avoid using their photograph.**

**If their photograph is used, we avoid naming the pupil.**

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

---

**Examples of how digital photography and video may be used at school include:**

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would cont you separately for permission, e.g. if your child won a national competition and wa named in local or government literature.

# The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show common courtesy online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

# Burlington Infant and Nursery School

## Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- 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. 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.
  This is currently: [*LGfL StaffMail / name system]*
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / school named contact*.
- I will not download any software or resources from the Internet 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 connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- 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.
- I will follow the school's policy on use of mobile phones / devices at school and *will not take into classrooms.*
- 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 *appropriate system or staff-only drive within school*.
- I will use the school's Learning Platform in accordance with school protocols.

- 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 agree and accept that any computer, laptop or mobile device loaned to me by the school, is provided primarily to support my professional responsibilities.
- I will only access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols.
- 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 will alert the Designated Safeguarding Lead if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to report any behaviour of other staff, which I believe may be inappropriate or concerning in any way, Designated Safeguarding Lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- Staff that have a teaching role only: I will embed the school's on-line safety / counter extremism curriculum into my teaching.

---

**User Signature**

I agree to abide by all the points above and 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 e-safety policies.

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

Signature Date

Full Name (printed)

Job title / Role

**Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature Date

Full Name (printed)