Burley Oaks PRIMARY SCHOOL
A MOORLANDS LEARNING TRUST ACADEMY
Belong, Believe, Achieve

ONLINE SAFETY HANDBOOK

May 2026 - May 2027

This handbook supplements the Trust's Online Safety policy with more detailed school-specific information so that all stakeholders are clear on the systems and processes required in order to keep everyone safe online.

CONTENTS

Education

Technical

Use of digital images and videos

Social media

Cameras and mobile devices

Communication

e Safeguarding Steering Group

EDUCATION

Pupils

Every person in school has a responsibility for online safety; to be safe and to keep others safe. Burley Oaks employs a specialist teacher as the computing lead who delivers the computing curriculum to all the children across the school. Promoting Online Safety is a key part of this role to ensure staff and children are vigilant and aware in all aspects of teaching and learning. Online Safety is a prominent feature in our work and remains a school priority in terms of training and a cycle of review, plan, action to be proactive and responsive to technological changes and therefore, potential dangers.

'Project EVOLVE' is the resource toolkit BOPS uses to deliver a comprehensive curriculum; it ensures both the coverage of the relevant statements from the UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" and the objectives stated in the National Curriculum:

Each year group from EYFS to Year 6 undertake lessons on the following strands:

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health Well-Being and Lifestyle
- Privacy and Security
- Copyright and Ownership

The content is delivered as short 'online safety warm ups' at the start of each computing lesson. The Project Evolve Knowledge Maps are used as an assessment tool.

At the start of each year, pupils are required to sign the 'Pupil Acceptable Use Agreement' which encourages them to adopt safe and responsible use, both within and outside school.

EDUCATION

Staff / Volunteers

All staff and volunteers receive Online Safety training as part of their induction and further training is provided at least annually. Every year, staff sign an acceptable use policy. The computing lead is provided with opportunities throughout the year to extend and refresh their online safety knowledge.

Governors

All Governors will take part in Online Safety training/awareness sessions at least annually.

Parents/Carers

The school provides Online Safety information and awareness to parents and carers through letters, newsletters and through the sharing of purchased online safety videos. There is a dedicated school webpage to support parents with key information and strategies.

TECHNICAL

INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

All users have clearly defined access rights to school technical systems and devices.

School-owned laptops that have been encrypted by the industry standard Windows 10 BitLocker are allowed access to the Burley Oaks network. All files are saved on OneDrive, which is accessed through two-factor verification. USB storage devices are not allowed to be used on our system.

All new users are provided with a username and password by the network manager/computing lead. Staff and children in KS2 and Year 2 have their own passwords. Year 1 and Reception use individual log-ins and cohort passwords. Users are responsible for the security of their username and password and are aware of the need to lock computers when they are not at them.

The school maintains and supports enhanced user-level filtering with the School Protect firewall filter, which screens inappropriate content. Logs are monitored by the network manager, and checks that the filter is working on all types of devices are completed and recorded every half term. A system is in place where staff can notify the network manager if something is found that should be blocked and also to request something to be unblocked.

Our school provides a Bring Your Own Device (BYOD) wireless network that allows personal devices to connect to the network without access to the school's data system.

The eSafeguarding software, SENSO, is installed on all devices on our system. It monitors keystrokes and records violations as they occur. These logs are checked regularly by our Designated Safeguarding Lead, who also receives real-time alerts for violations classified as high level.

Supply teacher log-in cards are issued by office staff, and the password is changed at the end of the day.

Trainee teachers are issued their own password and username, which are deleted from the system when their placement ends.

USE OF DIGITAL AND VIDEO IMAGES

Staff are encouraged to take digital/video images to support educational aims with school owned devices. Use of personal devices for this is not permitted. Images are deleted from the device once they have been uploaded onto the blogs or social media (see social media section) or downloaded onto the school network.

Images are only saved on the Media Drive of the network where there is a folder for each cohort. When a cohort of children leaves school all digital images of them are deleted from the drive.

Care is taken when taking digital/video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and, in some cases to protect them, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. Audiences are reminded about this policy at the beginning of services and performances.

Parental / legal guardians' consent is required for children's images to be used which is logged on the school MIS system.

SOCIAL MEDIA

School Accounts

Each year group has a blog which they update regularly. This is accessed through a username and password which is managed by the computing lead. A whole school X (formerly Twitter) account is also used.

The rules for the school's social media are:

- All content expressed on school social media accounts will not breach copyright, data protection or freedom of information legislation.
- Parental / legal guardians' consent is required for children's images to be used on social media.
- Members of staff uploading content to blogs, X and the school website will ensure that any photographs that are to be published have been checked with reference to records of parental permissions given.
- The school will never attach a name to an image, so that individuals are never identifiable.

Personal Accounts

Staff are reminded that their own personal social media accounts should not discuss school matters and that what they post and share reflects on the school. The school should never be brought into professional disrepute by a staff member's actions online or otherwise.

Staff are advised that their accounts are set to private.

CAMERAS AND MOBILE DEVICES

School Mobile Phones

The school has two mobile phones which are stored securely in the office and can be taken off site when staff are on school trips. The procedures for the use of these are:

Teachers understand that all the mobile devices are the property of the school and should be treated respectfully and with care. Teachers are asked to delete images / videos once they have been uploaded and this is checked termly by the computing lead.

Phones will be used for:

- Communicating with other members of staff, such as contacting the school office for assistance.
- Contacting parents, other staff members, third party companies and the school when on school trips.
- Contacting a parent in an emergency.
- Taking pictures and videos of pupils for school use, where consent has been obtained.
- Uploading photographs or videos to the social media platform, where consent has been obtained and in accordance with the Social Media Policy.

Staff Mobile Phones

Burley Oaks Primary School allows staff to bring in personal mobile telephones and devices for their own use. Under no circumstances would the school permit a member of staff to contact a current child or parent/guardian using their personal device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

To ensure the safety and welfare of all the children within our care, we operate a no mobile phone usage policy in the school, which means that staff must not use their own personal devices for taking photographs of the children. This policy is also to protect our staff members against possible allegations.

CAMERAS AND MOBILE DEVICES

Staff Mobile Phones - continued

Staff must not take their mobile phones out to check the time, messages, emails etc. where children are present. This should be done at break times, away from children, in the staffroom or an empty classroom.

Phones must be kept securely by staff and not left on display or unattended.

Parent / Helpers / Students / Visitors

All parent helpers/students/visitors etc. will be requested to follow the same rules as staff.

Pupils' Mobile Phones

Year 5 and 6 pupils are allowed to bring mobile phones into school once a consent form is signed. Phones are handed into the class teacher on arrival at school and then stored in the school office. These are returned to the classroom, by an adult, at the end of the day. The phones are turned off before entering the school grounds and turned back on once out of the school grounds.

The only exception to this rule would be where a mobile device is required for medical purposes, e.g. blood sugar monitoring and a separate agreement / system would be made in consultation with the headteacher.

Pupils' Smart Watches

Burley Oaks operates a no smart watches policy for children.

COMMUNICATION

Email

All staff are provided with a school email address which is part of the Outlook platform. Staff are aware that:

- It is understood by all parties that emails are not routinely monitored however, email on school systems can be monitored by SLT should this be thought necessary in any circumstances.
- Any digital communication with parents should be through school email, not through text or social media and should be composed in a professional manner.
- Teachers are not expected to respond to emails after 5pm or before 8am.
- If non teaching staff receive emails from parents or regarding our pupils, they must be shared with teachers and/or SLT as soon as possible.
- If an email received is threatening, inappropriate or concerning in anyway then this should be reported immediately to SLT.
- No staff member will open any attachments to emails, unless they know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programs.

ONLINE SAFETY STEERING GROUP

Burley Oaks has an e safeguarding steering group which meet on a half termly basis. It is made up of:

- Computing lead
- Network manager
- SLT and DSL
- Class teachers
- Support staff
- Governor

The objective of the group is to review, evaluate and develop our e safeguarding procedures. As part of each meeting's agenda, there are the following set items:

- A review of the number of Impero violations for that half term.
- A filtering report.
- Results of the most recent filtering test.
- Curriculum developments/improvements
- School improvement