Digital Technology Policy for Pupils

Guidelines for the use of Digital Technology

This policy is intended as guidelines on the correct use of Information Technology for pupils both inside and outside of school. Pupils receive E-Safety lessons appropriate to their age group from Year 3 onwards. Whilst at school, staff guide pupils in the correct use of information technology. Outside school, families have the same duty to guide children as they use digital technologies.

For further information on safeguarding, cyberbullying and online safety please refer to the school Safeguarding Policy.

Section 1: School IT Systems & Acceptable Use

The IT systems at Ballard are provided to support teaching and learning. Limited personal use of IT services are permitted, but pupils are expected to exercise sound judgement and use this privilege sensibly. Unreasonable or inappropriate use will constitute misuse of the facilities and sanctions will be imposed as such.

- Pupils should always ask permission before using any school IT resources
- IT Systems are not to be tampered with in any way. Any faults with school IT equipment should be reported to a member of the IT Department as soon as possible via the IT help email address. ithelp@ballardschool.co.uk
- Files of any type that could cause damage to the school system are not be downloaded or used on the school systems
- It is the responsibility of pupils to ensure any personal USB Memory sticks used in school computers have been scanned for viruses.

School Email

Pupils should take care when writing emails that they are written carefully and politely. When using email from a school email address, it is sent via school systems and therefore could impact upon the reputation of the school.

- Pupils from Year 3 onwards are provided with an email address. Email accounts are restricted to internal use only for Years 3- 5.
- Email communication between students and staff must be made via the school email system. The use of personal email accounts is not permitted.
- School email accounts may be configured on personal devices if desired.
- Chain letters, phishing attempts or other spam should be deleted immediately and are not be forwarded on.

Wireless Network

A wireless network is available across the school site. Personal laptops and mobile devices may be configured to use the wireless network. Access is granted by using standard Ballard user account credentials. If assistance is required to connect your device to the wireless network, please see a member of the IT Support Department.

Section 2: Internet Use

All pupils have prescribed internet access permissions that apply whilst accessing the internet whether it is via a school computer or any other device. Ballard has the facility to monitor internet use and in line with our safeguarding responsibilities and the prevent duty to protect children from radicalisation, reports are regularly run to monitor its correct use. Each pupil is accountable for their use of the internet. Ballard may exercise its right to investigate pupils' internet history including the interception of emails where it believes the school IT systems are being used inappropriately.

3G/4G Enabled Devices (Mobile Data)

Whilst in school, we recommend mobile data is switched off and if internet access is permitted and required, it is via our protected wireless network and internet connection.

It should be noted that ultimately, safe use of the internet lies with the individual and their ability to identify the risks that are presented before them. E-safety principles are fully embedded in our curriculum and taught appropriately to each year group.

Social Media

Social media (e.g. Facebook, Twitter, Instagram) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, and video sharing platforms such as You Tube have social media elements to them.

Ballard recognises the numerous benefits and opportunities which a social media presence offers. However, there are risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

Pupils are not permitted to use any form of social media in school without explicit permission from a member of staff. However, Ballard is mindful that pupils may use social media outside school and therefore promotes its safe use by adhering to the following guidelines.

- When communicating on-line, pupils should be aware of "stranger danger", pupils should not disclose or share personal information about themselves or others when on-line (this may include names, addresses, email addresses, telephone numbers, age, gender, educational details)
- Use and check privacy and security settings regularly to protect your information.
- Before posting personal photos, thought should be given as to whether the images are appropriate.
- Before posting images of other people, permission must be sought from the subject of the photo.
- When posting on social media, you should be mindful that you are broadcasting to the world. Be aware that comments expressed via social networking under the impression of a 'private conversation' may still end up being shared in a more public domain, even with strict privacy settings.
- Online behaviour should reflect the same standards that are expected when conversing face-to-face. What is inappropriate in the classroom should be deemed inappropriate online

- Pupils should be mindful that what they publish will be published for a long time. Future employers could locate even your earliest social media posts. Publishing any material that may damage the reputation of the school will always be dealt with as a serious matter.

Section 3: Mobile Devices

Ballard is aware of the numerous benefits of using personally owned technology at school and encourages its correct use to enrich pupils' education. This section is intended to ensure that pupils use their devices safely and effectively. Pupils from Years 3 to 5 are not permitted to bring any form of mobile device in to school. Pupils are provided with school owned, shared devices for lessons where needed.

Years 3 – 7- Mobile Phones

Pupils from Years 3 to 7 are not permitted to bring mobile phones to school. Should there be a need to phone home, a member of staff will make contact or a pupil may phone from the Reception office with permission from the staff there.

Years 8– 11-Mobile phones

Pupils from Year 8 to Year 11 may bring mobile phones to school but they must either be kept in their possession or safely secured in lockers during the course of the school day.

Mobile phones should always be switched off during school hours unless a member of staff has given permission for educational purposes. Any phone calls during the school day should only be made by using the school telephone system in school reception. Mobile phone calls or any form of messaging is not permitted during school hours, unless by explicit permission from a member of staff and then only for clear educational purposes.

BYOD Programme (Bring Your Own Device)

Pupils may bring their own device to school to aid with their education. Personal devices brought to school must be insured. Ballard accepts no responsibility for any damage or loss. The use of mobile devices including laptops is allowed during lesson time or study time and only when permitted by a member of staff. Devices should be used responsibly and appropriately for the task in hand. Inappropriate use will result in sanctions being imposed (such as the confiscation of the item for a period of time). Mobile devices must be used on battery power only as sockets may not be suitably positioned. It is the responsibility of the pupil to ensure their device is fully charged for the school day.

Devices deemed appropriate for school should meet the following criteria.

- Battery life to last the whole school day
- Personal devices should be a minimum of an iPad size
- Devices should be able to run Microsoft office
- Wi-Fi Enabled (no 3G/4G capability is requested)
- Email facility
- Print facility
- Anti-virus, depending on device

Digital Photos, Audio & Video Recordings

With the presence of mobile devices in school, most of which incorporate cameras along with audio and video recording facilities, pupils must be mindful of their responsibility to use their devices sensibly. Permission must always be obtained from the subject of the material if photos or audio/video recordings are to be taken and must only be used for educational purposes. Distributing or posting material taken in school to social media or other public channels is strictly forbidden.

Digital Music & Games

Pupils are only permitted to listen to music or play games on any device in school when explicit permission has been granted by a member of staff. Dedicated portable games consoles are not allowed in school.

Section 4: Account Security & Passwords

Each pupil at Ballard is responsible for their own user account. User account details are not to be shared under any circumstances. When typing in your password, take care that you are not being overlooked. If it is suspected that an account is being used fraudulently, reset the account password and see the IT Systems Manager.

Pupils from years 6 to 11 are required to set their own passwords which undergo an enforced password change at the beginning of each school year. If pupils forget their password, they should see a member of the IT department for a password reset.

Secure passwords are important for any user account. Passwords for the Ballard IT system must meet the following criteria:

- Passwords must have at least eight characters
- Passwords cannot contain the user name or parts of the user's full name
- Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols
- Passwords cannot be reused

Be aware when choosing a new password, other systems/accounts that rely on your school password will need updating with the new password. E.g. wireless network access or email accounts on mobile devices.

Section 5: Health & Safety

The following summarised guidelines, as published by the HSE (health and safety executive), should be followed where possible to achieve the optimum working position when using desktop computers.

Getting comfortable

- Forearms should be approximately horizontal and the user's eyes should be the same height as the top of the screen.
- Arrange the desk and screen to avoid glare, or bright reflections. This is often easiest if the screen is not directly facing windows or bright lights.

Using a keyboard and mouse

- A space in front of the keyboard can help you rest your hands and wrists when not typing
- Try to keep wrists straight when typing
- Position the mouse within easy reach, so it can be used with a straight wrist.

- Sit upright and close to the desk to reduce working with the mouse arm stretched.
- Move the keyboard out of the way if it is not being used.
- Support the forearm on the desk, and don't grip the mouse too tightly.
- Rest fingers lightly on the buttons and do not press them hard.

Reading the screen

- Make sure individual characters on the screen are sharp, in focus and don't flicker or move. If they do, the monitor may need servicing or adjustment.

Breaking up long spells of computer work helps prevent fatigue, eye strain, upper limb problems and backache. The following may help users:

- Stretch and change position.
- Look into the distance from time to time, and blink often.
- Change activity before users get tired, rather than to recover.
- Short, frequent breaks are better than longer, infrequent ones.

Section 6: Safety Advice for Pupils

General safety advice and guidelines for using the internet.

- Use caution when posting personal information online.
- Think carefully about what should be shared in public and what shouldn't
- When you choose a profile picture for a social networking website, avoid photos that could give strangers clues about where you live or where you go to school
- Remember that people on the internet are not necessarily who they say they are. Never share personal information with somebody you don't know.
- If somebody you don't know adds you as a friend or sends you an email, ignore them and delete their request or email.
- Should you ever receive any unpleasant material or something which makes you feel uncomfortable, report it to a teacher or your parents.
- Never meet in person anybody that you have met online without an adult that you trust and the permission from your parents
- Use strong passwords. A combination of letters, numbers and symbols are best and never share your passwords with anyone. If you suspect someone knows your password, then change it
- Do not open attachments from people you don't know, they could contain viruses
- If you are ever unsure of anything on the internet, do not be afraid to talk to your parents or teacher

Section 7: Advice for Parents

Some suggestions which parents may find helpful in order to try and encourage the safe use of the internet and social media with their children.

- Monitor your child/children's internet usage. Methods of monitoring and parental controls are supplied by most internet service providers to assist in the management of internet use at home.
- Open a clear line of communication for your child/children to know that they should come to you if something makes them feel uncomfortable.
- Ask to see your child/children's social media accounts on occasion.

- Setup your own social media accounts to learn more about how the sites work.
- Most mobile devices have the capability to have restrictions set up to only allow apps appropriate to a particular age group.

- Encourage your child/children to talk about their use of the internet with you and why they like the sites they do.
- Help your child to understand that some people lie online and that therefore it's better to keep online friends online. They should never meet up with any strangers without an adult they trust.
- Consider not allowing internet-enabled devices in your child's bedroom

The Child Exploitation and Online Protection Centre, CEOP, have a website which contains a comprehensive list of advice and resources to help to keep children safe online. https://www.thinkuknow.co.uk/parents/

Section 8: School sanctions

This policy is deemed as being covered by the pupil code of conduct (which is published on the school website and is in the pupil logbook) and in serious cases a pupil may be punished for inappropriate use under the Exclusions' Policy. The wrong use of IT in school, in addition to its use out of school which brings the school into disrepute or which causes another pupil, parent, staff member or alumnus harm or upset, can expect a firm response. At the lowest level this might mean the banning of the use of personal devices / IT equipment in school, the confiscation of items and the use of detentions to, at the highest level, exclusions and, if the law of the land is infringed, a report to the Police.

All pupils and parents are issued with this policy and it is intended that is it is read through together, in order that both parents and pupils have fully understood the document. The rules and guidelines in this policy are designed to ensure that IT is used safely and appropriately in the classroom and at home.

This policy will be reviewed regularly by the members of the IT Committee.

Document updated by **Mr A Harris, IT Systems' Manager** July 2017