ICT and Communication Systems Policy May 2018

Please also refer to the Data Protection Policy, the E-Safety Policy and the Staff Handbook/Code of Conduct.

POLICY STATEMENT

The Governing Body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material and that data is kept secure.

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and email and Internet facilities during their own time subject to such use:

1. Not depriving children of the use of the equipment and/or

2. Not interfering with the proper performance of the staff member's duties.

Whilst the school's ICT systems may be used for both work-related and for personal use, the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

This policy document is to be issued to all staff on its adoption by the Governing Body and to new staff when provided passwords giving access to the ICT network and/or with mobile phones.

Policy coverage

This policy covers the use by staff of all school owned ICT and communications equipment, examples of which include:

- Laptop and personal computers
- ICT network facilities
- Tablets and iPads
- Mobile phones and phone/computing hybrid devices
- Memory sticks (USB keys) and other physical and on-line storage devices,
- Image data capture and storage devices including cameras, camera phones and video equipment.

This list is not exhaustive.

The policy covers the use of all ICT and communications equipment provided for work purposes and equipment which is on loan to staff by the school for their personal or study use.

Use of School ICT Equipment including memory sticks and cameras

Staff who use the school ICT and communications systems:

- Must use it responsibly and must keep it safe.
- Must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries.
- Must report any known breach of password confidentiality to the Executive Headteacher or Business Manager as soon as possible.
- Must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems.
- Must report to the Executive Headteacher any vulnerabilities affecting child protection in the school's ICT and communications systems.
- Must not install software on the school's equipment, including freeware and shareware, unless authorised by the school's ICT Coordinator.
- Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures.
- Must ensure that it is used in compliance with this policy.
- Must not use a memory stick unless it is encrypted.
- Must delete photos every half term from cameras and must not take cameras out of the school.
- Must not download personal data onto their home PC or other device if accessing the Network remotely.

Any equipment provided to a member of staff is provided for their use only, and must not be shared. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

Email and internet and communications systems usage

The following uses of the school's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

1. To make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it.

2. To make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred.

3. For the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation.

4. For the publication and/or distribution of libelous statements or material which defames or degrades others.

5. For the publication of material that defames, denigrates or brings into disrepute the school and/or its staff, children and families.

6. For the publication and distribution of personal data without authorisation, consent or justification.

7. Where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination.

8. To participate in on-line gambling.

9. Where the use infringes copyright law.

10. To gain unauthorised access to internal or external computer systems (commonly known as hacking).

11. To create or deliberately distribute ICT or communications systems “malware”, including viruses, worms, etc.

12. To record or monitor telephone or e-mail communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below).

13. To enable or assist others to breach the Governors’ expectations as set out in this policy.

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

- Participation in “chain” e-mail correspondence (including forwarding hoax virus warnings)
- Pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)
- Access ICT facilities by using another person’s password, or to post anonymous messages or forge e-mail messages using another person's identity.
- Use of personal email accounts for business related to Lilycroft Nursery School.
- Sending unencrypted emails which include personal data about children, families or staff.

The above restrictions apply to the use of phones, emails, social media, text messaging, internet chatrooms, blogs, and personal websites (including personal entries on Facebook, Snap Chat and Instagram etc).

School website

Whilst the Governors aim to make the school website accessible to all, no personal information will be displayed, except for the staff list (names and room only). Contact details on the website will be:

- The school address
- The “office” e-mail address
- The school telephone number

The school website will not publish:

- Staff or pupil contact details
- The names of any pupils who are shown

Permission for the use of children’s images is sought during the home visit process prior to the child’s admission.

GDPR and Personal Data

Staff must take special care regarding recording, storing, sharing and destroying electronic documents and files that constitute "personal data" about children and families, including photos and videos. Personal data should never be emailed outside of the school's email network unless a secure email such as Galaxkey is used. See the Data Protection Policy for further guidance.

Use of mobile phones

Certain members of staff are issued with a work mobile phone. Under no circumstances, other than an emergency, should they be used to make personal calls.

Personal/work mobile phones must never be used by staff to take photographs within the school or whilst on visits to other schools unless permission has been given by the Executive Headteacher.

Personal mobile phones should be left in the lockers that staff are provided with or in locked drawers. They should not be used during working time.

Mobile phones may be used during lunch breaks, after work etc but only in the administration areas and the staffroom. If a member of staff has an emergency that requires them to access/use their mobile phone, they must request permission from a member of the SLT.

Social networking including the nursery Facebook page

We use lots of photographs and videos of children and families who come to nursery on posters, leaflets, in staff training and on our website and Facebook page. We hope that these are a source of pleasure and pride which enhance self-esteem for children and families.

We ask parents on the admissions form for permission to take photos and videos. If permission is given for us to take photos and videos, they may be used on any of our publicity materials. If you do not want us to take photos of you or your child please make sure that you let us know. We delete all Facebook posts within 2 months of posting.

It is recognised that staff are likely to use social networking sites in their recreational time on their own personal computers. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute. The adding of children and young people, parents and carers known only in a work context as 'friends' to a social networking site is prohibited. No member of staff should make comments about the children or school business, or post photos of children, on social networking sites. This includes (but is not limited to) Facebook, Whatsapp, Bebo, Twitter, Snapchat etc.

Cyberbullying

Legal definition (http://en.wikipedia.org): Cyberbullying is defined in legal glossaries as:

- Actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm another or others.
- Use of communication technologies for the intention of harming another person
- Use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or text messaging with the intention of harming another person.

The Governors/Executive Headteacher will immediately investigate any instances of cyberbullying.

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer (including e-mails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

Complaints procedure

- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Executive Headteacher.
- Complaints of a child protection nature must be referred to the named person(s) and dealt with in accordance to the school's Child Protection procedures
- As with other safeguarding issues, there may be occasions when the police must be contacted.

Appendix 1: Legal issues relevant to the use of ICT and communications equipment

Computer Misuse Act 1990

This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks are covered. Unauthorised access to a computer is the most likely offence within the Council. Only use machines/systems which you are authorised to use.

GDPR 2018

Individuals have rights about personal data recorded on computer and in manual files. An individual can request access to his personal data, this includes email and other electronic files. See the Data Protection Policy for further guidance.

Copyright, Design & Patents Act 1988

It is an offence to copy software without the author's permission. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. Some Internet sites will not let you copy material you find there. Take care.

The Defamation Act 1996

Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way that could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

Sex Discrimination Act 1975

Race Relations Act 1976

Disability Discrimination Act 1995

Protection from Harassment Act 1997

Accessing or distributing material which may cause offence to individuals or damage the Council's reputation may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

Human Rights Act 1998

The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. Under this Act a UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Obscene Publications Act 1959

All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item. The Council is the originator of the Bradford Internet & Intranet sites, or the Governing Body in the case of Voluntary Aided and Foundation schools.

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978;

Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Appendix 2: Policy and Guidance on School ICT and Communications Systems

PART 1: to be retained by staff member

This declaration refers to the Governing Body's policy and guidance on the use of ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the declaration below.

You should sign two copies of this document; this copy to be retained by you. The second copy (below) is to be detached and placed your personal file.

Declaration

I confirm that I have been provided with a copy of the school's policy on the use of the school's ICT and communications systems. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date: .....

✂----------

Policy and Guidance on School ICT and Communications Systems

PART 2: to be detached and placed on the employee's file

This declaration refers to the Governing Body's policy and guidance on the use of ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the declaration below.

You should sign two copies of this document; this copy is to be retained on your personal file.

Declaration

I confirm that I have been provided with a copy of the school's policy on the use of the school's ICT and communications systems. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date: .....

Appendix 3: Use of USB Memory Sticks, Cameras and Phones

Data Storage and Transfer

On no account should staff or children's data:

- Be stored on a personal computer or any other device
- Be transferred via email to a personal computer or other device
- Be saved on an unencrypted USB stick
- Be taken out of the building without prior agreement

Loss

The loss of a school issued memory stick, camera or mobile phone must be reported at once to the School Business Manager. Failure to do so may result in disciplinary action. The cost of a replacement will be £25 to be paid by the user.

Memory sticks

It is the school's policy that no USB memory sticks other than school USB memory sticks are allowed to be used. Staff can only use a memory stick for work purposes if:

- It has been issued by the school and is encrypted
- It is signed out to staff and returned when the staff member leaves.

Please note that data is wiped from the memory stick automatically after 6 failed password attempts. Therefore, please ensure you use a secure password you will remember.

NO PERSONAL USB MEMORY STICKS ARE TO BE USED.

Cameras

Cameras are issued to staff to be used as a resource to aid teaching, learning, monitoring and reporting on children's progress.

- Cameras are assigned to individual members of staff during the school day.
- Cameras are to be stored in bumbags provided by the school and worn during the school day.
- Cameras must be stored securely in school outside of school hours.
- Cameras must not be taken out of school – unless agreed by the Head of School eg for school trips
- Cameras must be reviewed each half term and all photos deleted.
- Staff must be up to date with any parent/carer requests re: photograph taking and usage.
- Printing of photographs must be in school only and collected from the printer immediately (any left at the end of each school session will be shredded).
- Improper use can result in cameras being taken away from staff.

Mobile phones

Work mobile phones are issued to staff who are based off-site, are away from the office for long periods of time or if they are doing a large number of home visits. Mobile phones must be password protected.

No personal information other than name and phone number should be stored on the mobile phone. If using a mobile phone to text parents, texts should be deleted within a week.

Mobile phones should NOT be used to take photos.

Mobile phones are also available to any staff doing a home visit, as part of our Lone Working Policy.

Appendix 3 cont'd: Use of USB Memory Sticks, Cameras and Phones

Name (please print):			
Start date:			
Confirmation	**Signed**	**Date**	**Returned**
I confirm that I understand the conditions detailed above.			**N/A**
I am in receipt of an encrypted memory stick issued by school.			
I am in receipt of a camera issued by school.			
I am in receipt of a mobile phone issued by school.			

Staff Leavers

In the case of staff leavers, school issued memory sticks, cameras and mobile phones must be returned to the HR Administrator during the Exit Interview, along with other items such as ID pass and access fob.